

# **BAB I**

## **PENDAHULUAN**

### **1.1 Latar Belakang**

Suatu instansi yang menggunakan sistem jaringan komputer, keamanan jaringan merupakan aspek krusial yang harus diperhatikan dalam menjaga integritas data, serta memastikan kesediaan layanan sistem untuk para pengguna (Gutama et al., 2022). Tanpa keamanan yang memadai, jaringan menjadi rentan terhadap berbagai jenis serangan siber yang dapat menimbulkan kerugian. Ancaman atau serangan siber kerap kali terjadi dalam dunia jaringan komputer, khususnya pada jaringan internet. Sasaran dan pola serangannya juga banyak dan beragam. Oleh karena itu, penerapan protokol keamanan jaringan yang efektif sangat penting untuk melindungi aset digital dan menjaga kelangsungan operasional.

Berbagai ancaman keamanan jaringan mendorong pentingnya regulasi untuk mengatur keamanan informasi dan jaringan. Di Indonesia, keamanan jaringan dan sistem informasi diatur dalam beberapa undang-undang, salah satunya adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang diperbarui dengan Undang-Undang Nomor 19 Tahun 2016. UU ini mengatur tentang perlindungan sistem elektronik, termasuk jaringan komputer, dari serangan siber seperti *hacking*, *malware*, dan serangan *Denial of service* (DoS). Selain itu, ada Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), yang menegaskan kewajiban penyelenggara sistem elektronik untuk memastikan keamanan jaringan mereka. Regulasi ini menekankan pentingnya penerapan standar keamanan untuk

menjaga integritas, kerahasiaan, dan ketersediaan data, yang pada akhirnya melindungi aset digital dan pengguna jaringan dari ancaman yang merugikan.

Perangkat yang rentan terhadap serangan siber pada sistem jaringan komputer adalah router (Haeruddin, 2021). Router menjadi target yang mudah diserang karena perannya yang sangat penting dalam menghubungkan jaringan lokal (LAN) dengan internet. Oleh karena itu seringkali router menjadi target bagi oknum peretas yang tidak bertanggung jawab. Pada negara berkembang perangkat router yang umum digunakan adalah router berbiaya terjangkau, router yang hemat biaya dan dapat berfungsi baik sebagai router untuk penggunaan di rumah maupun sebagai router utama dalam sebuah jaringan infrastruktur (Scholten, 2019). Salah satu jenis router yang memiliki biaya terjangkau yaitu Mikrotik, dari penelitian yang telah dilakukan oleh (Scholten, 2019) mengkaji karakteristik serangan siber pada router berbiaya rendah Mikrotik dengan memanfaatkan *honeypot* dan diperoleh data mengenai pola serangan seperti *Mikrotik Common Vulnerabilities and Exposures* (CVE), *Denial of service* (DoS), dan *Brute-Force Attacks*.

CVE (*Common Vulnerabilities and Exposures*) adalah sistem yang dipercaya secara global dan diterima oleh berbagai organisasi dan perusahaan untuk melacak kerentanan keamanan dalam perangkat lunak, termasuk perangkat Mikrotik. Pada tahun 2018, ditemukan sebuah celah keamanan pada perangkat Mikrotik yang diberi nama CVE 2018-14847 salah satu kerentanan paling terkenal yang pernah ditemukan pada Mikrotik. Serangan *Winbox Exploitation* memanfaatkan celah keamanan CVE-2018-14847 pada router Mikrotik (Haeruddin, 2021). Serangan *Winbox Exploitation* memungkinkan penyerang mendapatkan akses tidak sah ke router tanpa memerlukan otentikasi, yang dapat digunakan untuk mengubah

konfigurasi dan pengaturan keamanan. Selain itu, penyerang dapat mengambil data sensitif seperti kata sandi dan pengaturan jaringan dari file konfigurasi router. Dengan akses penuh, penyerang dapat mengendalikan seluruh router, menyebabkan gangguan operasional yang serius, termasuk memanipulasi lalu lintas jaringan. Dampaknya tidak hanya mengganggu layanan, tetapi juga membuka peluang bagi penyerang untuk meluncurkan serangan lain, seperti *Denial of service* (DoS).

Situs *cvedetails.com* sebuah *platform* yang mencatat data kerentanan CVE (*Common Vulnerability and Exposures*) memberikan data bahwa jenis penyerangan router mikrotik yang paling banyak terjadi dari tahun 2015 sampai dengan tahun 2024 ini adalah serangan *Denial of service* (DoS). Hal ini dikarenakan serangan DoS merupakan serangan yang sangat umum terjadi, oleh karena itu banyak peneliti yang melakukan simulasi dengan menggunakan jenis serangan DoS ini, kemudian melakukan pencegahan atau mitigasi terhadap serangan DoS pada hardware site maupun server (Rosihan & Muin, 2022). Serangan DoS merupakan jenis serangan yang umum menargetkan perangkat seperti server, web dan termasuk juga router Mikrotik. Serangan ini melibatkan banyak perangkat yang secara bersamaan membanjiri target dengan lalu lintas berlebihan, membuat sistem tidak mampu menampungnya. Serangan DoS (*Denial of service*) bertujuan untuk membuat jaringan router *down* atau tidak berfungsi, Akibat serangan ini, router tidak mampu memproses layanan dari pihak yang mempunyai otorisasi yang valid. Hal tersebut bisa mengganggu kegiatan operasional serta merugikan organisasi, baik secara materi seperti hilangnya pendapatan, maupun nonmateri seperti kerusakan reputasi atau gangguan pada proses bisnis yang penting (Jagad et al., 2020).

Menurut (Bahri, 2023) masih banyak masyarakat kita yang kurang edukasi dalam membuat *username* dan kata sandi yang kuat, sehingga menjadi sangat rentan terhadap peretasan. *Brute force attack* adalah ancaman presisten dan merugikan yang kerap dimanfaatkan oleh pihak ilegal untuk memperoleh akses ke perangkat jaringan terutama pada router mikrotik dengan mencoba berbagai kombinasi *username* dan *password* berulang-ulang. Metode ini mengandalkan uji coba terus-menerus hingga menemukan kombinasi yang tepat untuk masuk ke sistem. *Brute force attack* mengakibatkan akses ilegal ke jaringan, pencurian data sensitif, serta kerusakan pada integritas sistem secara keseluruhan. Dampak dari serangan ini bisa sangat merugikan, baik dari segi keamanan data maupun operasional. Oleh karena itu, penerapan keamanan jaringan yang tepat sangat penting untuk menjaga sistem agar tetap aman dari ancaman seperti ini.

Serangan *Winbox Exploitation* dapat memberikan akses tidak sah kepada penyerang dengan memanfaatkan kerentanan yang ada pada router Mikrotik (CVE 2018-14847). Sementara itu, *Brute force attack* menyebabkan penyerang mendapat akses ilegal dari upaya menebak kombinasi *username* dan kata sandi secara berulang-ulang pada router Mikrotik. Kemudian, *Denial of service* (DoS) dapat menghentikan layanan internet secara keseluruhan yang berpotensi merusak infrastruktur dan mengganggu operasional bisnis atau organisasi. Oleh sebab itu, sangat penting untuk melakukan upaya pencegahan dalam menghadapi serangan tersebut. Langkah pencegahan yang dapat dilakukan adalah dengan cara implementasi sistem keamanan yang kuat pada router Mikrotik melalui konfigurasi *firewall*, sehingga router Mikrotik lebih terlindungi dari berbagai ancaman ini. *Firewall* adalah salah satu *tools* yang efektif dalam meningkatkan perlindungan

jaringan komputer. Fungsinya adalah untuk mencegah akses yang tidak sah ke jaringan serta mengontrol lalu lintas yang diizinkan (Pratomo, 2023). Namun, untuk memastikan bahwa konfigurasi *firewall* yang diterapkan sudah tepat, diperlukan pengujian. *Penetration testing* merupakan metode pengujian yang sering diimplementasikan, metode ini memungkinkan kita untuk mengidentifikasi kelemahan dan memastikan bahwa router terlindungi dengan baik dari potensi serangan. (Rafay Baloch, 2017) menerangkan bahwa *Penetration testing* merupakan rangkaian teknik dan langkah-langkah yang diterapkan untuk menguji keamanan sistem suatu organisasi. Proses ini bermanfaat dalam menemukan celah keamanan yang ada di dalam organisasi dan menilai apakah *attacker* bisa memanfaatkan kerentanan tersebut untuk memperoleh akses tanpa izin.

Era digital saat ini menjadikan jaringan komputer di sekolah memiliki peran yang sangat krusial dalam mendukung berbagai aktivitas pendidikan (Sinaga et al., 2022). Jaringan komputer mempermudah proses belajar mengajar serta mendukung administrasi sekolah secara efisien. Meskipun jaringan komputer memberikan banyak manfaat, risiko keamanan yang menyertainya tidak boleh diabaikan. Tanpa adanya keamanan jaringan yang memadai, jaringan sekolah bisa saja mengalami ancaman seperti peretasan, atau serangan yang dapat mengganggu layanan internet. Ancaman seperti *Winbox Exploitation*, *Brute force*, dan *Denial of service* (DoS) adalah beberapa contoh serangan yang bisa mengakibatkan gangguan serius pada jaringan sekolah. *Winbox Exploitation* dan *Brute force* memberikan kesempatan bagi penyerang untuk memperoleh akses tanpa izin ke perangkat jaringan sekolah. Sementara, serangan *Denial of service* (DoS) dapat menyebabkan jaringan sekolah

lumpuh, membuat layanan internet tidak bisa diakses, dan menghambat proses pembelajaran.

SMA Negeri 1 Balongpanggang yang terletak di Kabupaten Gresik, Jawa Timur merupakan lembaga yang bergerak di bidang pendidikan. Sebagai institusi pendidikan, sekolah ini berperan dalam menyediakan layanan pembelajaran dan pengembangan siswa di tingkat menengah atas. Salah satu fasilitas yang tersedia di SMA Negeri 1 Balongpanggang adalah akses internet. Akses internet diberikan kepada semua warga sekolah, termasuk kepala sekolah, guru, karyawan, dan seluruh siswa. Fasilitas internet diharapkan dapat mendukung kegiatan belajar mengajar serta memenuhi kebutuhan administrasi sekolah. Berdasarkan hasil observasi dan wawancara yang telah dilakukan dengan Bapak Abdur Rosyid Amrullah, S.Kom. selaku guru TIK dan kepala laboratorium komputer pada tanggal 3 Oktober 2024, beliau menyebut bahwa sekolah ini masih belum menerapkan sistem keamanan jaringan, perancangan sistem jaringan sekedar difokuskan untuk dapat menghubungkan perangkat satu sama lain dan memberikan akses internet. Konfigurasi router Mikrotik yang diterapkan hanya fitur *hotspot* saja sebagai metode otentikasi dasar bagi pengguna yang ingin mengakses jaringan internet di sekolah. Dalam sesi wawancara tersebut beliau juga mengatakan bahwa jaringan sekolah tidak selalu berjalan dengan lancar seringkali terjadi permasalahan jaringan seperti koneksi yang tiba-tiba hilang atau *down*. Ketika peneliti bertanya terkait potensi terjadinya serangan *cyber crime* seperti *winbox exploitation*, *brute force*, dan *Denial of service* (DoS) beliau menyatakan bahwa serangan tersebut sangat mungkin terjadi, mengingat belum adanya sistem keamanan yang dapat mendeteksi dan mencegah dari serangan-serangan tersebut. Hal ini tentu sangat berbahaya

karena serangan-serangan tersebut dapat menghambat proses belajar mengajar dan menyebabkan gangguan operasional yang berdampak pada seluruh aktivitas sekolah yang bergantung pada jaringan internet.

Penelitian yang dilaksanakan oleh (Sediqy et al., 2023), yaitu mencegah serangan DoS, *Brute force*, dan *winbox exploit* terhadap router mikrotik melalui pembaruan dan penerapan *firewall* pada router. *Penetration testing* digunakan untuk menemukan kerentanan jaringan.

Penelitian sebelumnya yang relevan yaitu penelitian yang dilaksanakan oleh (Haeruddin, 2021), menerapkan uji penetrasi dan mengimplementasikan sistem keamanan dari serangan *Winbox Exploitation*, *Brute force*, serta *Denial of service*. Hasil pengujian menunjukkan bahwa untuk mencapai hasil optimal diperlukan beberapa langkah antara lain melakukan pembaruan sistem operasi router Mikrotik, pembatasan akses ke layanan Winbox, SSH, dan Web pada router Mikrotik, serta penerapan *firewall*.

Penelitian yang dilaksanakan oleh (Mamuriyah et al., 2024), tujuan penelitian ini adalah untuk menguji sistem keamanan jaringan dari serangan DDOS menggunakan pengujian penetrasi. Hasil dari penelitian ini metode pengujian penetrasi membuktikan bahwa sistem keamanan jaringan yang dirancang efektif dalam mendeteksi dan mencegah serangan DDOS

Penelitian yang dilaksanakan oleh (Rosihan & Muin, 2022), tujuan penelitian ini untuk meningkatkan keamanan jaringan terhadap router mikrotik dengan menerapkan metode *Penetration testing* dengan beberapa serangan diantaranya adalah *Exploitation*, *Brute force*, dan DDoS. Hasil penelitian menunjukkan bahwa dari beberapa pengujian yang dilakukan, ditemukan sejumlah kerentanan pada

jaringan Informatika Unkhair. Hal ini menggaris bawahi pentingnya kesadaran yang lebih tinggi dari administrator jaringan terhadap keamanan sistem. Oleh karena itu, peneliti merekomendasikan penerapan *firewall* dan menutup *port* yang tidak digunakan, karena *port* tersebut dapat dimanfaatkan oleh penyerang untuk mengakses sistem Mikrotik.

Berdasarkan hasil observasi, wawancara dan penelitian yang relevan tersebut, peneliti menetapkan untuk melakukan penelitian di SMAN 1 Balongpanggang dengan mengamankan jaringan dari serangan *Winbox Exploitation*, *brute force* dan *Denial of service* (DoS) dengan judul “Implementasi dan Pengujian Keamanan Router Mikrotik Terhadap Serangan Siber Menggunakan *Firewall* dan *Penetration Testing*”.

## **1.2 Rumusan Masalah**

Rumusan masalah dari penelitian ini adalah:

1. Bagaimana implementasi keamanan pada Router Mikrotik untuk mengatasi serangan siber *Winbox Exploitation*, *Brute force*, dan *Denial of service* (DoS)?
2. Bagaimana metode *penetration testing* digunakan dalam pengujian keamanan Router Mikrotik terhadap serangan siber *Winbox Exploitation*, *Brute force*, dan *Denial of service*?

## **1.3 Tujuan Penelitian**

Tujuan dari penelitian ini adalah:

1. Mengimplementasikan *firewall* sebagai sistem keamanan pada router Mikrotik untuk mengatasi serangan siber *Winbox Exploitation*, *Brute force*, dan *Denial of service* (DoS).

2. Menggunakan metode *penetration testing* dalam pengujian keamanan router Mikrotik terhadap serangan siber *Winbox Exploitation*, *Brute force*, dan *Denial of service* (DoS).

#### 1.4 Spesifikasi Produk yang diharapkan

Spesifikasi produk yang diharapkan peneliti dalam penelitian ini adalah sebagai berikut :

1. Router Mikrotik yang dikembangkan mampu memblokir dan memitigasi serangan yang memanfaatkan kelemahan pada layanan *Winbox* yaitu *Winbox Exploitation*.
2. Router Mikrotik memiliki mekanisme untuk mencegah upaya *login* yang berulang dengan kata sandi atau *username* yang salah (*Brute force Attack*)
3. Router Mikrotik yang dikembangkan mampu memitigasi serangan *Denial of service* (DoS) jenis DNS TCP SYN *Flood Attack* yang berpotensi mengganggu kinerja jaringan

#### 1.5 Batasan Penelitian

Batasan masalah dari penelitian ini adalah:

1. Implementasi dilakukan pada jaringan yang ada di sekolah SMA Negeri 1 Balongpanggang.
2. Penelitian ini berfokus pada implementasi dan pengujian keamanan Router Mikrotik.
3. Penelitian dibatasi pada tiga jenis serangan, yaitu *Winbox Exploitation*, *Brute force*, dan *Denial of service* (DoS) jenis DNS TCP SYN *Flood Attack*.
4. Pengujian keamanan dilakukan dengan menggunakan metode *Penetration testing*.

5. *Tools* uji serangan Mikrotik yang dipakai antara lain *Exploitation Script*, *Hydra*, dan *Hping3*.

## **1.6 Pentingnya Penelitian Pengembangan**

Adapun manfaat yang diharapkan dari penelitian ini adalah sebagai berikut :

### **1.6.1 Manfaat Teoritis**

Penelitian ini diharapkan dapat memberikan kontribusi teori dalam bidang keamanan jaringan, khususnya terkait implementasi dan pengujian keamanan router mikrotik terhadap serangan siber menggunakan *firewall* dan *penetration testing*. Hasil penelitian ini dapat menjadi referensi dan pendukung bagi penelitian-penelitian selanjutnya yang berfokus pada keamanan jaringan dan teknologi mikrotik.

### **1.6.2 Manfaat Praktis**

1. Bagi peneliti, Penelitian ini memberikan kesempatan kepada peneliti untuk memperdalam pemahaman dan keterampilan dalam implementasi dan pengujian keamanan mikrotik menggunakan metode *penetration testing*. Penelitian ini juga meningkatkan pemahaman peneliti tentang cara menangani serangan siber yang sering terjadi, seperti *Winbox Exploitation*, *Brute force*, dan *Denial of service* (DoS), khususnya dalam konteks Router Mikrotik.
2. Bagi sekolah, implementasi keamanan pada Router Mikrotik di sekolah dapat membantu administrator jaringan dalam mencegah serangan yang mungkin masuk. Dengan demikian, jaringan sekolah akan lebih stabil, tidak mudah *down*, dan kegiatan belajar mengajar berbasis internet dapat berjalan dengan lancar tanpa gangguan dari serangan siber.

## 1.7 Definisi Istilah

1. Keamanan jaringan adalah aspek yang sangat penting dalam jaringan komputer, yang bertujuan untuk melindungi sistem dari berbagai kelemahan dan ancaman yang dapat menyebabkan kerugian, seperti kehilangan data, kerusakan pada sistem server, dan kehilangan aset berharga di sebuah organisasi.
2. Routerboard adalah perangkat keras yang menggunakan sistem operasi RouterOS. Perangkat ini berfungsi sebagai server jaringan komputer yang andal dan dapat mengelola jaringan komputer, baik melalui LAN maupun WLAN.
3. Mikrotik adalah sistem operasi berbasis perangkat lunak yang digunakan untuk mengubah komputer menjadi router dalam suatu jaringan. Sistem operasi ini didasarkan pada Linux dan berfungsi sebagai fondasi untuk *network* router. Mikrotik sangat ideal digunakan dalam mengelola jaringan komputer, baik untuk skala kecil maupun besar.
4. *Winbox Exploitation* merupakan serangan yang mengeksploitasi kerentanan keamanan CVE-2018-14847 pada router Mikrotik, yang memungkinkan penyerang mengakses router tanpa memerlukan otentikasi. Hal ini memungkinkan mereka untuk membaca file konfigurasi dan bahkan mengubah pengaturan sistem. Eksploitasi ini sangat berbahaya karena dapat memberikan penyerang kendali penuh atas router.
5. *Brute force attack* adalah metode yang melibatkan percobaan berulang untuk menebak kombinasi nama pengguna dan kata sandi hingga menemukan yang tepat. Dalam serangan ini, penyerang secara otomatis mencoba berbagai variasi

kemungkinan hingga mereka berhasil mendapatkan akses yang sah. Serangan ini seringkali menargetkan sistem dengan kata sandi yang lemah atau akun yang tidak memiliki perlindungan yang memadai.

6. Serangan *Denial of service* (DoS) merupakan serangan yang umum dilakukan dalam dunia kejahatan *cyber*. Tujuan utama dari serangan ini adalah untuk membuat jaringan router tidak dapat beroperasi, sehingga tidak bisa merespons permintaan dari pengguna yang berwenang.
7. *Penetration testing* merupakan proses menguji keamanan sistem, jaringan, atau aplikasi dengan cara mensimulasikan serangan dari pihak luar. Tujuannya adalah untuk mengidentifikasi kerentanan serta menguji sejauh mana sistem dapat bertahan terhadap ancaman dan serangan.