BAB II

TINJAUAN PUSTAKA DAN DASAR TEORI

2.1 Tinjauan Pustaka

Penelitian ini menggunakan beberapa sumber pustaka yang berhubungan dengan kasus atau metode yang akan diteliti, Diantaranya adalah sebagai berikut :

Arief Indriarto Haris, Budhi Riyanto, Farry Surachman dan Ardito Adi Ramadhan (2022) dalam penelitiannya melakukan analisa pengamanan jaringan router terhadap serangan DoS. Kemudian ditemukan bukti bahwa serangan DoS memberikan dampak pada router dimana konsumsi resource target mengalami peningkatan yang sangat signifikan terutama dari sisi CPU.

Yudi Mulyanto dan Akbar Algi Fari (2022) dalam penelitiannya melakukan analisis analisis keamanan login router MikroTik dari serangan *Brute-Force*. Didapatkan hasil serangan *Brute-Force* menyebabkan jaringan menjadi lambat dan semua pengguna jaringan akan terputus dari jaringan tersebut.

Roby Nurbahri, Yuhandri dan Gunadi Widi Nurcahyo (2023) dalam penelitiannya melakukan analisis metode *Port Knocking* untuk keamanan router. Didapatkan hasil bahwa administrator jaringan dapat melakukan blokir pada port yang rentan pada serangan antara lain Winbox (tcp 8291), SSH (tcp 22), Telnet (tcp 23), dan webfig (tcp 80) dengan menggunakan metode *Port Knocking*.

Budi Jaya, Yuhandri Yunus dan Sumijan (2020) dalam penelitiannya melakukan peningkatan keamanan router terhadap serangan DoS. Didapatkan hasil

bahwa *Firewall Filter* dapat menyaring paket data yang masuk pada jaringan router sedangkan *Firewall Raw* berfungsi untuk memblokir *IP Address* yang dicurigai mengirim paket data tidak wajar pada jaringan router.

Bayu Santosa dan Ali Akbar Rismayadi (2022) dalam penelitiannya mengimplementasikan metode *Firewall filtering* untuk keamanan jaringan LAN. Didapatkan hasil bahwa *Firewall filtering* dengan *rule acces list* mengatur perizinan jaringan berdasarkan *IP Address* sehingga dapat membokir situs dewasa yang ada pada jaringan LAN dengan menggunakan *rule acces list* tersebut.

Perbandingan dari penelitian ini dengan penelitian sebelumnya adalah memiliki kesamaan dalam meneliti kinerja router terhadap serangan DoS dan *Brute-Force* dengan menggunakan *Firewall*, namun metode yang digunakan dalam penelitian ini adalah metode IDS dengan menggunakan *Firewall rules* serta menambahkan notifikasi melalui WhatsApp Bot. Penelitian ini juga menambahkan serangan *cyber* lain yaitu *Brute-Force* untuk menguji keamanan router dengan metode yang diteliti.

Tabel 2.1 Tinjauan Pustaka

No	Penulis	Objek	Metode	Keterangan
1.	Arief dkk (2022)	Pengamanan Jaringan Router MikroTik dari Serangan DoS dan Pengaruhnya Terhadap Performansi	PPDIOO *(Prepare, Plan, Design, Implement, Operate* dan *Optimize)*	Jurnal Penelitian
2.	Yudi dkk (2022)	Analisis keamanan *login* router MikroTik dari serangan *Bruteforce*	*Penetration Testing*	Jurnal Penelitian
3.	Roby dkk (2023)	Analisis Penggunaan Metode Port Knocking pada Sistem Keamanan Jaringan Komputer	*Port Knocking*	Jurnal Penelitian
4.	Budi dkk (2020)	Peningkatan Keamanan Router MikroTik	*Live Forensic*	Jurnal Penelitian

No	Penulis	Objek	Metode	Keterangan
		Terhadap Serangan Denial of Service (DoS)		
5.	Bayu dkk (2022)	Implementasi Keamanan Jaringan LAN Menggunakan MikroTik Dengan Metode Firewall Filtering	*Firewall Filtering*	Jurnal Penelitian
6.	Yang diusulkan	Implementasi Sistem Keamanan Jaringan dengan Deteksi Serangan Denial of Service dan Brute-Force pada Router MikroTik dengan Notifikasi melalui WhatsApp	IDS (*Intrusion Detection System*)	Jurnal Penelitian

2.2 Dasar Teori

2.2.1 Jaringan Komputer

Jaringan kompter didefinisikan sebagai sekupulan komputer yang saling terhubung satu dengan yang lainnya menggunakan media berupa kabel (*wire*) maupun tanpa kabel (*wireless*) sehingga memungkinkan interaksi, bertukar data serta berbagi piranti bersama seperti *printer, scanner*, dan perangkat lain diantara komputer tersebut, (Yuliandoko, H., 2018).

Berdasarkan jumlah komputer yang terkoneksi dalam sebuah jaringan maka jaringan komputer terbagi menjadi 2 jenis :

- *Point to Point*, menghubungkan dua komputer secara langsung.
- *Multiple Point*, menghubungkan lebih dari dua komputer dengan menggunakan saluran atau jaringan secara bersama.

Sedangkan berdasarkan luas jangkauan jaringan dan jumlah komputer yang terlibat dalam jaringan maka jaringan komputer terbagi menjadi:

- LAN (*Local Area Network*) yaitu jaringan komputer dengan cakupan area yang terbatas seperti gedung perkantoran atau laboratorium dengan jangkauan tidak lebih dari 10 Km.
- MAN (*Metropolitan Area Network*) merupakan perluasan dari LAN dengan versi yang lebih besar dimana MAN dapat mencakup kantor-kantor persahaan yang letaknya berdekatan atau sebuah kota dengan jarak maksimum kira-kira 80 km.
- WAN (*Wide Area Network*) yaitu jaringan dengan jangkauan area geografis yang paling luas dibandingkan dengan LAN dan MAN. WAN dapat mencakup jaringan antar pulau, negara, benua atau lebih dikenal dengan sebutan internet.

2.2.2 Sistem Keamanan Jaringan

Rangkaian aturan dan konfigurasi untuk meningkatkan perlindungan dalam jaringan komputer. Keamanan jaringan merupakan sistem yang bekerja untuk pencegahan aktivitas yang tidak diinginkan dengan melakukan identifikasi pengguna yang tidak memiliki hak akses dalam suatu jaringan, (Al Fikri, K., & Djuniadi, D., 2021).

Sistem keamanan komputer menargetkan berbagaimacam serangan siber yang kemudian menghalangi masuknya ancaman tersebut ke dalam jaringan. Tujuan dari sistem keamanan jaringan adalah untuk melindungi integritas, keamanan, aksesibilitas data dan jaringan komputer.

2.2.3 Firewall

Sistem atau perangkat jaringan yang memantau dan menyaring lalu lintas jaringan berdasarkan aturan keamanan (*security rules*) yang telah ditetapkan.

Firewall bertugas sebagai pos keamanan jaringan yang mencegah akses tidak sah masuk ke dalam jaringan. Hal ini dilakukan untuk mencegah ancaman baik dari virus maupun serangan siber yang dapat mengakibatkan kerugian. (Wicaksono, D., & Widiasari, I. R., 2022).

Firewall adalah suatu kombinasi antara perangkat keras (*hardware*) dan perangkat lunak (*software*) yang berperan menjadi pemisah di antara jaringan komputer menjadi dua atau lebih untuk menjaga keamanan data. Berikut beberapa jenis *firewall* yang umum digunakan pada perangkat MikroTik:

- *Firewall Filter:* Memungkinkan admin jaringan untuk mengatur aturan-aturan untuk memfilter dan mengatur lalu lintas yang melewati router, baik lalu lintas yang masuk maupun keluar. (Mulyana, A., & Suprianto, A., 2023).
- *Firewall RAW*: Memungkinkan admin jaringan untuk mengatur aturan *firewall* yang diterapkan pada paket data sebelum proses koneksi dijalankan. Ini memungkinkan penggunaan aturan-aturan khusus sebelum paket diproses oleh *firewall filter* utama. (Rokhman, M. N., Rizaldy, E. F., Abdullah, N., & Puspitasari, N. F. (2023).
- *Firewall Mangle*: memungkinkan admin jaringan melakukan *marking* atau penandaan pada suatu paket data tertentu. Paket data yang telah ditandai ini nantinya dapat digunakan oleh beberapa fitur yang ada pada router MikroTik. (Hamza, S., 2022).
- *Firewall Layer 7 Protocol*: Memungkinkan admin jaringan untuk mengidentifikasi dan memblokir lalu lintas berdasarkan protokol aplikasi

tingkat atas (Layer 7) seperti HTTP, FTP, SMTP dan NFS. (Husnaini, M., Bagye, W., & Ashari, M., 2019).

2.2.4 MikroTik RouterBOARD

RouterBOARD merupakan perangkat keras yang didesain dan diproduksi oleh perusahaan MikroTik asal Latvia menggunakan RouterOS sebagai sistem operasinya. RouterBoard mempunyai komponen seperti PC, tetapi mempunyai ukuran yang lebih kecil seperti *Processor, RAM, ROM* dan *Memory Flash*, dan hanya menggunakan Sistem Operasi RouterOS yang khusus diproduksi oleh MikroTik.

RouterBOARD ini digunakan untuk mengatur dan mengelola jaringan, seperti mengatur akses internet, mengelola *bandwidth*, menghubungkan jaringan lokal dengan jaringan publik, dan lain sebagainya.

Salah satu faktor yang mempengaruhi performa router MikroTik adalah *resource* CPU (*Central Processing Unit*) *Load*. Dalam kondisi normal, *resource* CPU *Load* MikroTik router berada antara 3-9%. Namun ketika MikroTik router diserang, mengakibatkan CPU *Load* pada router bisa mencapai nilai 80-100% sehingga mengakibatkan router *down* dan tidak dapat melayani *request user* lainnya. MikroTik router dapat dikatakan efektif dan efisien ketika nilai persentase CPU *Load* dibawah atau bernilai 55%. (Haris, Arief Indriarto, et al., 2022)

2.2.5 Denial of Service

DoS (Denial of Service) adalah jenis serangan *cyber* yang mencegah pengguna sah mengakses komputer atau jaringan. Serangan DoS melibatkan

pengiriman *request* secara terus menerus ke server target sehingga membebani *bandwidth* server secara berlebihan. *Fake traffic* yang dikirimkan peretas ini mengakibatkan server target tidak dapat merespon atau mengalami *crash*. Serangan DoS bukan dirancang untuk menangkap atau informasi sensitif, yang dapat dijual untuk mendapatkan keuntungan. Sebaliknya, serangan DoS dimaksudkan untuk mematikan atau mengganggu sistem organisasi dengan menyebabkan hilangnya waktu dan sumber daya secara signifikan pada layanan yang ditargetkan. (Andoyo, A., Angraeni, E. Y., & Khumaidi, A., 2021).

Ada dua metode umum serangan DoS yaitu *flooding services* dan *crashing services*. *Flooding services* terjadi ketika sistem menerima terlalu banyak lalu lintas untuk di-*buffer* oleh server sehingga menyebabkannya melambat dan terhenti. Serangan *flooding* yang populer meliputi:

1. *Ping of Death*

Serangan *Ping of Death* adalah jenis serangan DoS di mana penyerang mengirimkan paket ping yang berukuran lebih besar dari ukuran standar (65.535 *byte*) ke komputer target. Paket yang sangat besar ini dapat membuat sistem target tidak dapat memproses paket tersebut dengan benar, sehingga menyebabkan *crash* atau kinerja yang sangat lambat.

2. *Syn Flood*

Jenis serangan yang memanfaatkan kerentanan dalam protokol TCP/IP. Serangan ini dimulai dengan penyerang mengirimkan banyak permintaan koneksi SYN palsu ke server atau perangkat target. Penyerang tidak pernah menyelesaikan

proses koneksi, yang mengakibatkan alokasi sumber daya yang signifikan pada server target dan akhirnya menyebabkan penolakan layanan kepada pengguna yang sah.

Proses *SYN flood* terjadi ketika penyerang mengirim permintaan koneksi SYN dalam jumlah besar, melebihi kapasitas server untuk menanggapi dan menangani permintaan tersebut. Hal ini membuat server tidak dapat memproses permintaan koneksi dari pengguna yang sah. Dengan demikian, server menjadi tidak responsif atau bahkan dapat mengalami kegagalan.

3. *Remote Controlled Attack*

Aktivitas yang mengendalikan beberapa jaringan lain untuk menyerang suatu target. Jenis serangan ini memiliki konsekuensi serius karena besarnya *bandwidth* server penyerang. Peretas memiliki kendali bebas atas target dan dapat bersembunyi di balik server penyerang.

4. *UDP Flood*

Jenis serangan yang menargetkan protokol UDP (*User Datagram Protocol*) Pada serangan ini, penyerang mengirimkan sejumlah besar paket UDP palsu ke target dengan tujuan membanjiri sumber daya jaringan, menyebabkan ketidakmampuan sistem untuk menangani lalu lintas yang tinggi dan memproses permintaan yang sah. Karena protokol UDP tidak memerlukan koneksi yang terjaga, serangan ini dapat dengan mudah membanjiri sistem target tanpa memerlukan proses *handshake* yang rumit.

UDP flooding biasanya memanfaatkan kelemahan dalam implementasi protokol UDP, di mana server atau perangkat target tidak dapat membedakan antara lalu lintas yang sah dan lalu lintas yang berasal dari serangan. Dengan membanjiri sistem dengan lalu lintas palsu, penyerang dapat membuat sumber daya jaringan menjadi tidak tersedia bagi pengguna yang sah.

5. Serangan *Smurf*

Serangan jaringan dimana penyerang membanjiri jaringan target dengan paket *ICMP Echo Request* (permintaan *ping*) palsu. Serangan ini memanfaatkan protokol ICMP (*Internet Control Message Protocol*) dan biasanya dilakukan dengan menggunakan teknik *spoofing IP*. Dalam serangan ini, penyerang mengirimkan permintaan *ping* palsu dengan alamat sumber yang dipalsukan sehingga tampak berasal dari alamat target yang diserang. Kemudian permintaan *ping* tersebut dikirimkan ke jaringan yang di-*hosting* oleh router yang memiliki kemampuan *broadcast*.

2.2.6 Brute-Force

Serangan *Brute-Force* melibatkan upaya berulang dengan mencoba semua kemungkinan kombinasi kata sandi serta *username* secara berurutan. Serangan ini memiliki tujuan untuk mendapatkan akses tidak sah ke akun, sistem, atau data yang terproteksi. (Permana, A. A., et al., 2023).

Serangan *Brute-Force* memanfaatkan ketidakseimbangan antara kekuatan kata sandi yang lemah dengan kemampuan dan sumberdaya komputasi yang semakin meningkat. Cara kerja serangan *Brute-Force* adalah dengan menggunakan

program atau *script* yang akan mengulang kombinasi kata secara otomatis otomatis secara berurutan hingga menemukan yang benar.

2.2.7 Intrusion Detection System

IDS (*Intrusion Detection System*) adalah sistem yang dirancang khusus untuk mendeteksi aktivitas mencurigakan di jaringan komputer atau sistem komputer. Sistem ini memantau lalu lintas jaringan dan aktivitas sistem untuk mendeteksi tanda-tanda serangan atau aktivitas ilegal. (Purnama, T., 2023).

Setiap aktivitas atau pelanggaran ilegal sering kali dicatat secara terpusat menggunakan sistem SIEM (*Security Information and Event Management*) atau diberitahukan kepada suatu administrasi.

Intrusion Detection System diklasifikasikan menjadi lima yaitu:

1. *Network Intrusion Detection System* (NIDS)

Jenis IDS yang dirancang untuk memonitor dan menganalisis lalu lintas jaringan secara keseluruhan guna mendeteksi aktivitas mencurigakan, ancaman potensial, atau serangan siber yang mungkin terjadi. NIDS memeriksa paket data yang beredar di jaringan, menganalisis header, dan konten paket untuk mengidentifikasi pola yang mencurigakan atau sesuai dengan pola serangan yang telah diketahui sebelumnya.

2. *Host Intrusion Detection System* (HIDS)

Jenis IDS yang diimplementasikan di dalam *host* atau server tertentu untuk memonitor dan menganalisis aktivitas pada *host* tersebut. HIDS bertujuan untuk

mendeteksi tanda-tanda aktivitas mencurigakan, serangan, atau perubahan tidak sah yang terjadi pada sistem operasi, aplikasi, atau file di *host* tersebut.

3. *Protocol-based Intrusion Detection System* (PIDS)

Jenis IDS yang berfokus pada analisis protokol jaringan untuk mendeteksi ancaman atau serangan terhadap lalu lintas jaringan berdasarkan pelanggaran protokol yang ditentukan. Sistem ini bekerja dengan memantau aktivitas lalu lintas jaringan untuk mencari pelanggaran aturan atau protokol yang dapat menunjukkan adanya serangan atau aktivitas yang mencurigakan.

4. *Application Protocol-based Intrusion Detection System* (APIDS)

Jenis IDS yang difokuskan pada analisis protokol aplikasi yang digunakan oleh perangkat lunak atau layanan di jaringan. APIDS bertujuan untuk memantau, menganalisis dan mendeteksi aktivitas mencurigakan atau serangan terhadap protokol aplikasi yang digunakan dalam lingkungan jaringan.

5. *Hybrid Intrusion Detection System*

Menggabungkan berbagai teknik dan pendekatan dari berbagai jenis IDS untuk meningkatkan kemampuan deteksi dan respons terhadap ancaman keamanan. Dengan menggabungkan elemen-elemen dari berbagai IDS, sistem hibrida dapat menawarkan tingkat perlindungan yang lebih komprehensif dan efektif terhadap serangan siber dan aktivitas mencurigakan di dalam jaringan.

2.2.8 WhatsApp

WhatsApp adalah aplikasi pesan instan yang memungkinkan pengguna untuk mengirim pesan teks, panggilan suara, panggilan video, serta berbagi berbagai jenis file seperti gambar, video, dan dokumen. WhatsApp pertama kali dirilis pada tahun 2009 oleh WhatsApp Inc. kemudian diakuisisi oleh Facebook Inc. pada tahun 2014.

Fitur utama WhatsApp meliputi:

- Pesan Teks: Pengguna dapat mengirim pesan teks secara instan kepada individu atau dalam grup.
- Panggilan Suara dan Video: Aplikasi ini memungkinkan pengguna untuk melakukan panggilan suara dan video secara gratis melalui koneksi internet.
- Pengiriman File: Pengguna dapat mengirim dan menerima berbagai jenis file, termasuk gambar, video, dokumen, lokasi, dan kontak.
- Enkripsi *End-to-End*: WhatsApp menggunakan enkripsi end-to-end untuk melindungi privasi pengguna, sehingga hanya pengirim dan penerima yang dapat membaca isi pesan.
- Status dan Cerita: Pengguna dapat membagikan status singkat atau cerita dengan kontak mereka, yang akan hilang setelah 24 jam.
- Grup *Chat*: Pengguna dapat membuat grup chat untuk berkomunikasi dengan beberapa orang sekaligus.

WhatsApp hadir di berbagai platform, termasuk Android, iOS, Windows Phone, dan desktop. Aplikasi ini telah menjadi salah satu aplikasi komunikasi

paling populer di dunia karena kemudahannya digunakan, fitur yang lengkap, serta kemampuannya untuk beroperasi di berbagai jenis perangkat.

2.2.9 Twilio

Twilio adalah perusahaan teknologi yang menyediakan platform komunikasi cloud yang memungkinkan pengembang untuk membangun dan mengintegrasikan berbagai fitur komunikasi, seperti pesan teks, panggilan suara, panggilan video, dan layanan komunikasi lainnya ke dalam aplikasi mereka. Twilio menyediakan berbagai API (*Application Programming Interface*) dan layanan yang memungkinkan pengembang untuk menambahkan fungsionalitas komunikasi ke aplikasi mereka dengan mudah.

Beberapa produk dan layanan utama yang ditawarkan oleh Twilio meliputi:

- *Twilio Programmable Messaging*: memungkinkan pengembang untuk menyampaikan pesan teks secara global.
- *Twilio Programmable Voice*: memungkinkan pengembang untuk mengintegrasikan panggilan suara ke dalam aplikasi mereka.
- *Twilio Programmable Video*: platform yang memungkinkan pengembang untuk membangun pengalaman panggilan video interaktif.
- *Twilio SendGrid*: layanan email cloud yang membantu pengembang dan perusahaan mengelola komunikasi email mereka dengan pelanggan.
- *Twilio Flex*: platform pengalaman pelanggan yang fleksibel dan dapat disesuaikan untuk pusat kontak.

Twilio telah menjadi salah satu platform yang memungkinkan berbagai perusahaan dan organisasi untuk meningkatkan interaksi mereka dengan pelanggan melalui berbagai saluran komunikasi yang inovatif. Dengan API (*Application Programming Interface*) yang mudah digunakan dan dukungan yang kuat, Twilio telah menjadi pilihan utama bagi banyak pengembang dan organisasi untuk memperluas kemampuan komunikasi aplikasi mereka.