BAB II
Tinjauan Pustaka

2.1. Landasan teori

2.1.1. Serangan DDoS

Serangan DDoS adalah bentuk serangan untuk membuat layanan online menjadi down atau tidak bisa diakses oleh pengguna [1], sementara itu Budi Jaya menjelaskan bahwa DdoS merupakan salah satu serangan terhadap situs, jaringan, *router*, dan *server* yang sangat sering terjadi termasuk pada *router* mikrotik. Serangan DoS bertujuan untuk membuat jaringan *router* down sehingga tidak mampu melayani permintaan *user* yang memiliki hak akses yang sah [2].

2.1.2. SYN flood

SYN *flood* merupakan serangan penolakan layanan dimana penyerang dengan cepat memulai koneksi ke *server* target tanpa menyelesaikan koneksi yang telah dibuat sampai *server* target kehabisan *resource* karena harus menunggu koneksi yang belum selesai [5], [6].

2.1.3. UDP flood

UDP *flood* merupakan tipe serangan DDoS yang didesain untuk membuat sistem, *server*, bandwidth, atau mesin tidak dapat permintaan pengguna yang sah. Dikarenakan UDP adalah protocol yang tidak memiliki sesi, serangan UDP *flood* sangat efektif dan hanya membutuhkan sedikit *resource* untuk dijalankan [7].

2.1.4. HTTP flood

HTTP *flood* merupakan salah satu serangan DDoS yang didesain untuk membanjiri *server* dengan *HTTP request* sampai *server* target penuh dengan *request* dan tidak bisa merespon *traffic* yang normal [8].

2.1.5. DNS flood

DNS *flood* adalah tipe serangan DDoS dimana penyerang membanjiri sebuah DNS *server* dengan tujuan untuk mengganggu DNS menemukan domain yang dituju. Dengan mengganggu resolusi DNS, serangan DNS *flood* bisa mengganggu website, API, atau kemampuan aplikasi web dalam merespon trafik yang asli [9].

2.1.6. Smurf attack

Smurf attack merupakan serangan DDoS dimana penyerang mencoba membanjiri *server* target menggunakan paket ICMP dengan membuat request kepada satu atau lebih komputer dalam jaringan menggunakan alamat IP palsu dari perangkat tersebut [10].

2.1.7. Firewall

Firewall merupakan perangkat yang bertugas utnuk memantau lalu lintas jaringan yang masuk atau keluar dan memutuskan apakah paket data diijinkan atau diblok berdasarkan aturan khusus yang telah ditentukan [11]. *Firewall* juga merupakan mekanisme yang berada di dalam *Operating System* yang bertujuan untuk melindungi jaringan dengan efektif, dengan menerapkan aturan utnuk menyaring, membatasi, atau bahkan menolak aktifitas di dalam jaringan berdasarkan aturan yang sebelumnya telah dikonfigurasi [12], [13], [14], [15], [16], [17], [18].

2.1.8. Mikrotik

Router mikrotik merupakan *router* yang mencakup berbagai fitur handal di dalamnya namun dengan harga yang cukup terjangkau, salah satunya adalah fitur *firewall* untuk menghadapi ancaman serangan siber [6], [12], [19], [20]. Mikrotik juga memiliki sistem operasi yang disebut dengan *router*OS, *router*OS dapat menjadikan komputer biasa menjadi *router* network yang mencakup berbagai fitur seperti *firewall*, *routing*, *point-to-point*, *hotspot*, dan masih banyak lagi [21], [22].

2.1.9. LUCID

LUCID adalah *software* yang digunakan untuk mendeteksi DDoS berbasis CNN yang dapat digunakan dengan sumber daya yang terbatas. CNN yang digunakan mengenkapsulasi *learning* aktifitas jaringan yang berbahaya dari lalu lintas agar dapat mengidentifikasi pola DDoS tanpa mempedulikan posisi sementaranya [23].

2.1.10. Mausezahn

Mausezahn adalah *software* untuk *generate network traffic* dengan cepat yang ditulis menggunakan Bahasa C, hal ini mengijinkan pengguna untuk membuat hampir semua jenis paket. Projek ini digabungkan dengan *netsniff-ng toolkit* setelah pengembang yang asli meninggal pada 25 Juni 2011, dan berlanjut dikembangkan disana [24].

2.1.11. Hping3

Hping3 adalah *tool* jaringan yang dapat mengirimkan paket ICMP/TCP/UDP kustom dan menunjukkan balasan dari target layaknya ping dengan balasan ICMP. Hping3 menangani fragmentasi dan bentuk serta ukuran paket, dan dapat digunakan untuk mengirim file dalam protokol yang didukung [25].

2.1.12. Slowloris

Slowloris adalah tipe *software* serangan DoS yang dapat membuat satu mesin untuk melumpuhkan mesin web *server* lain dengan bandwidth dan efek samping dari *port* yang tidak bersangkutan secara minimal. Slowloris bekerja dengan cara menjaga banyak koneksi yang tersambung ke web *server* agar tetap terbuka dan menahannya selama mungkin [26].

2.2. Kajian Pustaka

Tabel 2.1 Penelitian terdahulu

Penulis	Judul	Metode	Hasil	Improvisasi
A. Rodiah Machdi (2021)	Analisa dan Impelementasi Sistem Keamaman Jaringan *Intrusion Detection System* (IDS) Berbasis Mikrotik	Implementasi IDS berbasis mikrotik terhadap 6 serangan DoS, yaitu SYN *flood*, UDP *flood*, ICMP *flood*, Smurf, Port Scan.	Hasil pada penelitian yang dilakukan oleh Agustini, memiliki akurasi 100% pada deteksi serangan namun hal tersebut bergantung terhadap konfigurasi ambang batas.	Improvisasi yang dilakukan pada penelitian ini adalah penambahan mitigasi serangan DDoS
Rana et all (2020)	An Effective Mechanism to Mitigate Real-Time DDoS Attack	Algoritma klasifikasi SVM pada SNORT IPS untuk mendeteksi dan mitigasi serangan DDoS	Hasil Pada penelitian yang dilakukan oleh Rana, tingkat deteksi mencapai 97.9% akurasi dari yang awalnya 91% dengan konfigurasi default.	Improvisasi yang dilakukan pada penelitian ini adalah tidak menggunakan bantuan pihak ketiga dalam mitigasi serangan DDoS karena membutuhkan *resource* lebih
Nuroji (2023)	Penerapan *Instrusion*		Hasil pada penelitian yang dilakukan oleh	Improvisasi pada penelitian ini adalah

	Detection and Prevention System (IDPS) pada Jaringan Komputer sebagai pencegahan serangan *Port-Scanning*		nuroji terbukti mencegah *port-scanning* namun tidak mencegah serangan DDoS sama sekali.	penggunaan perangkat dengan spesifikasi yang lebih umum dipakai pada LAN dan juga meningkatkan *firewall* agar dapat mengantisipasi serangan DDoS
A. N. Hairun, M. R. Katili, R. Takdir, and M. S. Tuloli (2023)	Penerapan *firewall* di *router* OS mikrotik pada aplikasi *e-rapor*	Penerapan *firewall* mikrotik *via* NAT untuk mitigasi serangan DoS pada aplikasi *e-rapor*	Pada penelitian yang dilakukan oleh hairun, teknik mitigasi yang digunakan adalah menggunakan NAT dan hasilnya mencapai 80%	Improvisasi pada penelitian ini adalah serangan yang digunakan menggunakan DDoS dan serangan yang digunakan juga lebih bervariasi seperti UDP *flood*, HTTP *flood*, DNS *flood*, dan *Smurf attack*.
B. Jaya, Y. Yuhandri, and S. Sumijan (2020)	Peningkatan Keamanan *Router* Mikrotik Terhadap Serangan *Denial of Service* (DoS)	Analisis serangan DoS menggunakan *live forensic* serta peningkatan keamanan *router* mikrotik menggunakan *firewall filter* dan *firewall raw* (*software*) dan menonaktifkan tombol *reset* (*hardware*)	Hasil pada penelitian yang dilakukan oleh budi jaya, teknik yang digunakan juga membutuhkan *firewall raw* dan juga menonaktifkan tombol reset. Namun hasil nya dapat menurunkan penggunaan CPU sebanyak 46%.	Improvisasi pada penelitian ini adalah penambahan serangan, yakni syn *flood*, udp (semua *port*) *flood*, http *flood*, dan *smurf attack*. Serta penambahan *custom* setting pada *firewall* dimana *user* bisa mengatur tingkat kerapatan trafik yang diperbolehkan untuk masuk dan keluar dari jaringan.

Pada tabel 2.1 dijelaskan beberapa penelitian terdahulu yang menjadi referensi penelitian ini. Penelitian yang dilakukan oleh Agustini et all adalah sumber ide dari penelitian ini, dan peneliti memutuskan untuk menambahkan mitigasi serangan DDoS dikarenakan penelitian hanya terbatas sampai deteksi serangan.

Teknik mitigasi serangan DDoS yang digunakan terinspirasi dari penelitian yang dilakukan oleh Rana et all, dimana algoritma klasifikasi yang digunakan memiliki tingkat akurasi deteksi yang tinggi, namun hal tersebut dicapai pada IPS yang jarang dijumpai pada jaringan LAN. Sebagai penggantinya *custom firewall* digunakan dengan konfigurasi yang menyerupai IDS/IPS.

Penelitian yang dilakukan Nuroji memberikan inspirasi untuk membuat *router* mikrotik sebagai IDPS, namun spesifikasi yang digunakan lebih rendah karena mikrotik yang digunakan oleh Nuroji memiliki spesifikasi yang tidak umum untuk digunakan pada jaringan LAN.

Penelitian Hairun et all memberikan gambaran dari tujuan penelitian yang akan dilakukan, yakni jaringan LAN seperti di sekolah, warnet, café, dll. Namun karena serangan yang digunakan hanya satu, maka pada penelitian ini ditambahkan agar memiliki variasi.

Penelitian Budi et all memberikan inspirasi untuk melakukan mitigasi secara *live*, namun pada penelitian ini, konfigurasi seperti menonaktifkan tombol *reset* tidak digunakan karena *reset router* secara fisik umumnya hanya dilakukan oleh *admin* jaringan dan *router* juga biasanya terletak jauh dari jangkauan pengguna.