BAB II

LANDASAN TEORI

2.1 Tinjauan Pustaka

Untuk mendukung penelitian ini, Penulis menggunakan beberapa *Literature* yang berkaitan dengan judul dan pokok bahasan pada penelitian. Adapun *Literature* yang dipergunakan dapat ditinjau pada Tabel 2.1.

Tabel 2. 1 Literature Review

No. Literature	Penulis, Tahun	Judul
Literature 01	(NURILAHI *et al.*, 2022)	Penerapan Metode *Naïve Bayes* pada *Honeypot Dionaea* dalam Mendeteksi Serangan *Port Scanning*
Literature 02	(Listyawati, Widjajarto and Kurniawan, 2022)	Implementasi dan Analisis Profil Sistem Pada Virtualisasi Paloalto *Firewall* Berdasarkan Metrik Sumber Daya Komputasi
Literature 03	(Mulyanto and Algi Fari, 2022)	Analisis Keamanan *Login Router* Mikrotik Dari Serangan *Brute Force*Menggunakan Metode *Penetration Testing*
Literature 04	(Christian, 2019)	Analisis Sistem Pengamanan Akses Autentikasi Jaringan dengan Metode *Port* Knocking dan Action *Tarpit* pada *Router* Mikrotik

Literature 05	(Marzuki, 2019)	Perancangan dan Implementasi Sistem Keamanan Jaringan Komputer Menggunakan Metode *Port* Knocking Pada Sistem Operasi *Linux*

2.1.1 Tinjauan Terhadap Literatur 01

Sesuai penelitian yang sudah dilakukan oleh (NURILAHI *et al.*, 2022) dengan judul "Penerapan Metode *Naïve Bayes* pada *Honeypot Dionaea* dalam Mendeteksi Serangan *Port Scanning*". Penulis mengulas tentang peningkatan serangan terhadap jaringan komputer yang terjadi tiap tahun dan konsekuensinya yang mengakibatkan gangguan pada layanan. Penelitian ini menggunakan *Dionaea Honeypot*, yakni jenis *Honeypot* Interaksi Rendah, untuk mengevaluasi serangan yang didasarkan pada teknik *Port Scanning*. Data log yang dikumpulkan selama pengujian dianalisis menggunakan metode *Naïve Bayes*. Hasil analisis menunjukkan bahwa penerapan metode *Naïve Bayes* berhasil dalam mengklasifikasikan potensi serangan berdasarkan teknik *Port Scanning*. Selain itu, data pemetaan *Port Scanning* dengan menggunakan aplikasi *Nmap* mengindikasikan adanya 359 *port* yang terbuka. Hasil uji klasifikasi menggunakan perangkat lunak *WEKA* dan metode *Naïve Bayes* menunjukkan tingkat akurasi sebesar 86,2%, dengan nilai presisi rata-rata sebesar 0,885%, *recall* sebesar 0,862%, dan *F-measure* sebesar 0,849%.

Dengan demikian, kesimpulan dari penelitian ini adalah bahwa penerapan *Honeypot* Interaksi Rendah, khususnya *Dionaea Honeypot*, dalam mendeteksi serangan *Port Scanning* terbukti berhasil. Hasil data *log* yang dianalisis menggunakan metode *Naïve Bayes* mampu mengklasifikasikan data *log* serangan *Port Scanning* dengan baik. Selain itu, kinerja *Dionaea Honeypot* juga terbukti efektif dalam menangani serangan *Port Scanning*.

2.1.2 Tinjauan Terhadap Literature 02

Sesuai penelitian yang sudah dilakukan oleh (Listyawati, Widjajarto and Kurniawan, 2022) dengan judul Implementasi dan Analisis Profil Sistem pada *Virtualisasi Paloalto Firewall* sesuai Metrik sumber Daya Komputasi. Dalam

percobaan ini, serangan *DDoS SYN flood* menggunakan *Kali Linux* digunakan sebagai pelaku serangan, sementara *Paloalto Firewall* di virtualisasi untuk melindungi jaringan *web* di *Ubuntu Network* menjadi target serangan. Dalam penelitian ini, ada dua skenario pengujian yang berbeda, yaitu pengujian layanan *HTTP* yang diizinkan *(HTTP allow*) dan pengujian layanan *HTTP* yang diblokir *(HTTP block)* dengan spesifikasi memori *Paloalto* pada *RAM* 5,5 GB dan *RAM* 8 GB.

Hasil eksperimen menunjukkan bahwa saat sumber daya komputasi dimanfaatkan secara maksimal selama serangan, penggunaan *CPU* mencapai rata-rata 95,8%. Peningkatan kedua terjadi pada penggunaan memori dengan rata-rata persentase sebesar 44%, dan jumlah sesi serangan mencapai 138.682. Berdasarkan analisis hasil, dapat disimpulkan bahwa karakteristik virtualisasi *Paloalto Firewall* cenderung bersifat linier, dengan peningkatan yang linier terjadi saat serangan dengan berbagai jumlah paket. Mayoritas hasil profil sistem *Firewall Paloalto* sesuai dengan pengujian layanan *HTTP* yang diizinkan (*HTTP allow*) maupun yang diblokir (*HTTP block*), dengan penggunaan *CPU* mencapai puncaknya pada 95,8%. Peningkatan kedua terjadi pada penggunaan sumber daya komputasi, khususnya memori, dengan tingkat penggunaan mencapai 44%, dan jumlah sesi serangan tertinggi mencapai 138.682.

2.1.3 Tinjauan Terhadap Literature 03

Berdasarkan penelitian yang telah dilakukan oleh (Mulyanto and Algi Fari, 2022) dengan judul Analisis Keamanan *Login Router* Mikrotik Dari Serangan *Brute Force* Menggunakan Metode *Penetration Testing*. Penelitian ini menerapkan metode *penetration testing* dengan tujuan untuk menganalisis kerentanan keamanan pada proses *login* pada *Router* Mikrotik yang terdapat di SMKN 2 Sumbawa. Dalam uji serangan (*trial attack*) yang dilakukan, penelitian ini menggunakan metode *Brute Force*. Hasil penelitian menunjukkan adanya celah keamanan pada halaman *login Router* Mikrotik yang dapat dieksploitasi dengan menggunakan serangan *Brute Force*, yang terbukti dengan berhasil memperoleh *username* dan *password* login untuk *Router* Mikrotik. Temuan akhir dari penelitian ini memberikan solusi untuk mencegah serangan *Brute Force*, yang dapat menjadi pertimbangan bagi administrator jaringan dalam meningkatkan keamanan *Router*.

Berdasarkan analisis hasil, dapat disimpulkan bahwa penelitian ini menggunakan metode *Penetration Testing* untuk mengidentifikasi celah keamanan pada *Router* Mikrotik RB-750 R3. Hasil serangan *Brute Force* yang dilakukan oleh peneliti terhadap jaringan di SMKN 2 Sumbawa menyebabkan kinerja jaringan menjadi lambat dan pengguna jaringan terputus. Setelah menyadari kerentanan keamanan, peneliti melakukan tindakan pencegahan dengan menambahkan skrip *Brute Force* ke dalam terminal *Winbox* yang terhubung dengan *Router* Mikrotik RB-750 R3.

2.1.4 Tinjauan Terhadap Literature 04

Berdasarkan penelitian yang telah dilakukan oleh (Christian, 2019) dengan judul Analisis Sistem Pengamanan Akses Autentikasi Jaringan dengan *Metode Port Knocking* dan *Action Tarpit* pada *Router* Mikrotik. Dalam penelitian ini, peneliti merancang konfigurasi hak akses pengguna pada *Port* dengan menggunakan Mikrotik *Router* serta menguji keamanan melalui metode *Port knocking* dan tindakan *Firewall* Tarpit. Metode *Port knocking* adalah teknik yang sementara menutup akses ke *Port. Port knocking* yang diterapkan pada Mikrotik *Router* ini bisa diakses melalui *Winbox* dan juga menggunakan layanan *web* pada *Webfig Winbox* yang telah disediakan oleh Mikrotik *Router.*

Hasil evaluasi oleh peneliti menunjukkan bahwa kinerja metode *Port knocking* sangat baik, di mana serangan *Brute Force* tidak berhasil menemukan username dan password untuk layanan Port tersebut. Hasil pengujian *scanning Port* menunjukkan bahwa tahap *scanning* berjalan dengan baik, dengan status *Port* yang disaring (*filtered),* yang berarti izin harus diberikan terlebih dahulu sebelum mengakses *Port* tersebut. Berdasarkan pengujian *scanning Port*, metode *Port knocking* dan tindakan Tarpit menghasilkan evaluasi yang baik, di mana *Port knocking* mampu mengurangi dan membingungkan serangan pada *Port FTP*, *SSH,* dan *HTTP.*

Kinerja *Port knocking* dan Tarpit mengakibatkan aplikasi *Bitvise SSH Client* atau layanan login jarak jauh tidak dapat melakukan *login* setelah melakukan *ping,* dan bahkan sebelum melakukan *ping,* aplikasi *Bitvise SSH Client* tetap tidak dapat melakukan *login.* Sebagai alternatif, administrator harus masuk melalui fitur *WINBOX* (antarmuka grafis yang disediakan oleh Mikrotik). Tidak ada

serangan yang berhasil dilakukan pada *Port* 8291, yang merupakan *Port Winbox* untuk mengakses sistem Mikrotik. Namun, ada metode lain selain mengakses *Port Winbox*, yaitu dengan mengakses *Port SSH* dan *HTTP*, karena *Winbo*x juga dapat diakses melalui *SSH* dan tersedia melalui layanan *web*.

2.1.5 Tinjauan Terhadap Literature 05

Berdasarkan penelitian yang telah dilakukan oleh (Marzuki, 2019) yang berjudul Perancangan dan Implementasi Sistem Keamanan Jaringan Komputer Menggunakan Metode *Port Knocking* Pada Sistem Operasi *Linux*. Fokus utama penelitian ini adalah pada sistem keamanan jaringan terhadap serangan yang dapat mengganggu atau merusak jaringan. Studi kasus dalam penelitian ini adalah jaringan *SSH* yang beroperasi di *Port* 22, karena layanan *SSH* umumnya menjadi target utama serangan oleh para penyerang. Metode keamanan yang diterapkan dalam penelitian ini adalah metode *Port knocking*. Prinsip kerja metode ini adalah jaringan akan menerima upaya koneksi dari klien ke *Port* tertentu yang telah ditentukan sebelumnya, setelah itu *firewall* akan mendeteksi upaya tersebut dan memberikan izin kepada klien untuk mengakses jaringan.

Setelah klien selesai mengakses jaringan, *firewall* akan kembali menutup akses ke jaringan, sehingga jaringan tidak dapat diakses kembali. Dalam penelitian ini, jaringan berhasil melindungi layanan-layanan yang ada dengan mengintegrasikan aturan firewall dengan program *Port knocking* yang digunakan. Lebih lanjut, tanpa memberikan ketukan yang sesuai, klien tidak dapat menggunakan layanan pada jaringan.

Berdasarkan hasil penelitian yang dilakukan, dapat disimpulkan bahwa sistem yang dirancang mampu meningkatkan tingkat keamanan dalam proses autentikasi ke jaringan, karena *Port* tidak terbuka secara bebas untuk publik. Metode *Port knocking* efektif dalam meningkatkan keamanan di sisi jaringan, karena klien harus memberikan "ketukan" ke *Port* tertentu untuk dapat mengakses layanan *SSH*.

2.2 Keaslian Penelitian

Adapun beberapa hal yang menjadi pembeda antara penelitian yang dilakukan penulis dengan penelitian yang sudah dilakukan sebelumnya sebagaimana terlampir di tabel tinjauan pustaka, antara lain adalah:

1. Penelitian ini berfokus pada implementasi sistem pencegahan terhadap serangan *Port Scanning*, *Distributed Denial of Service (DDOS)* dan *Brute Force* menggunakan *Firewall Tarpit* pada *Router* Mikrotik.
2. Sistem yang dibuat menggunakan *Tools-Tools* dari *Kali Linux* yaitu *Nmap, Pentmenu* dan *Hydra.*

2.3 *Kali Linux*

Kali Linux adalah sistem operasi berbasis Debian *Linux* yang dikembangkan *oleh Offensive Security*. *Kali Linux* hampir memiliki kemiripan seperti sistem operasi berbasis *Linux* lainnya,namun *Kali Linux* mempunyai *Tools* bawaan untuk pengujian keamanan digital (Fldr *et al.*, 2022)

2.4 *Virtualbox*

Virtualbox Oracle VM Virtualbox atau yang sering kita disebut dengan *Virtualbox* merupakan salah satu perangkat lunak yang saat ini dikembangkan oleh *Oracle*. *Virtualbox* berfungsi untuk melakukan virtualisasi sistem operasi. *Virtualbox* dapat digunakan untuk mengeksekusi sistem operasi tambahan di dalam sistem operasi utama (Fldr *et al.*, 2022)

2.5 Mikrotik

MikroTik adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi *Router network* yang handal, mencakup berbagai fitur yang dibuat untuk IP*network* dan jaringan *wireless,* cocok digunakan oleh ISP, *provider hotspot,* & warnet (Ardhitya, 20019)

2.6 *Router*

Router adalah perangkat jaringan yang digunakan untuk menghubungkan beberapa jaringan *(network*). Dalam jaringan yang lebih kompleks, *Router* digunakan untuk memilihkan jalan bagi paket data untuk mencapai komputer tujuan.

2.7 *Port Scanning*

Port Scanning merupakan salah satu serangan yang cukup berbahaya, teknik ini dapat memetakan karakteristik, *resources* serta mendeteksi *Port* yang terbuka pada sistem yang ada pada target, serangan ini dapat memberikan informasi-informasi penting pada suatu sistem atau host untuk kemudian diteruskan dengan serangan yang lebih lanjut. Serangan *DDOS* atau *Distributed Denial of Service* merupakan serangan yang dapat melumpuhkan target hingga tidak dapat beroperasi untuk beberapa waktu.

Serangan *Port Scanning* adalah serangan yang dilakukan dengan mencari *port* yang terbuka pada suatu jaringan untuk mengetahui layanan apa saja yang tersedia. Dalam konteks *firewall* tarpit pada router MikroTik menggunakan *Kali Linux*, serangan *Port Scanning* dapat dicegah dengan cara mengelabuhi aplikasi *Port Scanning* menggunakan *firewall* tarpit. Berikut adalah beberapa cara untuk mencegah serangan *Port Scanning* menggunakan *firewall* tarpit pada *router* MikroTik:

- Menggunakan *firewall* tarpit pada *router* MikroTik untuk menunda koneksi masuk dari sumber daya penyerang sampai kelelahan dalam koneksi yang tidak berguna
- Menambahkan *rule* pada *firewall* filter untuk menambahkan alamat IP penyerang ke dalam daftar hitam *(blacklist*) jika terdapat aktivitas *Port Scanning* yang mencurigakan
- Menandai alamat IP penyerang kemudian di-drop menggunakan fitur *firewall* pada router

Dengan menerapkan tindakan pencegahan tersebut, serangan *Port Scanning* dapat dicegah dan keamanan jaringan pada *router* MikroTik dapat terjaga.

2.8 *Brute Force*

Menurut Sinaga dalam bukunya yang berjudul *"Python Cryptography", Brute Force* adalah suatu teknik *cryptanalytic* dengan cara menebak kunci pas secara terus menerus, jika kunci yang dibangkitkan salah maka program akan mencoba kunci lain secara terus menerus hingga menemukan kunci yang tepat. akan digunakan untuk mendekripsi dan menampilkan pesan asli. Melalui Teknologi Informasi", *Brute Force* adalah metode *hacking* yang dilakukan dengan cara mencoba login berulang *Kali* hingga *password* berhasil ditebak, baik secara manual maupun otomatis *(robot). Protect* akan membatasi jumlah kesalahan *password* untuk durasi tertentu (Mulyanto and Algi Fari, 2022).

Serangan *Brute Force* adalah taktik serangan yang mencoba semua kombinasi *password* yang mungkin guna mendapatkan akses ke sistem atau jaringan. Dalam konteks penggunaan *firewall* tarpit pada *router* MikroTik dengan *Kali Linux*, serangan *Brute Force* dapat dihindari melalui beberapa tindakan, seperti menonaktifkan layanan yang tidak diperlukan pada router untuk mengurangi risiko serangan, mendeteksi alamat IP penyerang dan menghentikannya dengan fitur *firewall* pada *router*, serta menerapkan tarpit pada *firewall* untuk memperlambat koneksi yang berasal dari sumber daya penyerang hingga mencapai tingkat kelelahan yang tidak berguna. Salah satu contoh konfigurasi *firewall* pada router MikroTik untuk mencegah serangan *Brute Force* adalah dengan menambahkan aturan pada *firewall* filter untuk memasukkan alamat IP penyerang ke dalam daftar hitam (*blacklist)* apabila terdapat lebih dari 3 upaya *login* yang gagal pada *port SSH*. Selain itu, aturan juga dapat diterapkan untuk menandai alamat IP penyerang ketika terjadi upaya *login* yang gagal pada percobaan kedua dan ketiga. Melalui tindakan pencegahan ini, serangan *Brute Force* dapat ditekan dan keamanan jaringan pada *router* MikroTik dapat dipertahankan.

2.9 *DDOS*

DDOS attack atau *Distributed Denial of Service* merupakan serangan *cyber* dengan cara mengirimkan *fake traffic* atau lalu lintas palsu ke suatu sistem atau *network* secara terus menerus. Dampaknya, *network* tersebut tidak dapat mengatur seluruh *traffic* sehingga menyebabkan *down. Port Scanning, DDOS* dan *Brute*

Force merupakan kombinasi serangan yang sangat berbahaya, *Port Scanning* dapat memetakan kelemahan yang ada pada sistem, contohnya adalah dengan melihat *Port* yang terbuka, sedangkan *DDOS* dapat mengeksploitasi *Port* yang terbuka tersebut untuk dapat dibanjir trafficnya dengan *fake traffic* yang dapat melumpuhkan *network* target.

Perbedaan antara serangan *DOS* dan *DDOS* dijelaskan sebagai berikut:

1. Serangan *DOS* dilakukan oleh penyerang tunggal, sedangkan serangan *DDOS* melibatkan lebih dari satu mesin penyerang.
2. Tujuan dari kedua serangan ini sama, yaitu membuat aplikasi, layanan, atau mesin tidak tersedia.
3. Serangan *DOS* dan *DDOS* dilakukan dengan cara membanjiri lebih banyak permintaan daripada yang dapat ditangani, menggunakan sumber daya, atau memproses sedemikian rupa sehingga permintaan yang sah/legal tidak dapat ditangani.
4. Serangan *DDOS* memiliki jangkauan yang lebih luas dan dapat menargetkan semua jenis industri dan perusahaan dengan semua ukuran di seluruh dunia, sedangkan serangan *DOS* kebanyakan menyerang bisnis kecil hingga menengah yang tidak memiliki sumber daya yang besar.

Dengan demikian, perbedaan utama antara *DOS* dan *DDOS* adalah pada jumlah mesin penyerang yang terlibat dalam serangan tersebut.(Khairulah and Herdianto, 2023)

2.10 *Firewall Tarpit*

Firewall Tarpit merupakan salah satu action pada menu *Firewall* filter, fungsi dari action *Tarpit* tersebut adalah untuk melakukan drop suatu packet data, namun tetap dapat menjaga koneksi *TCP* yang masuk,sehingga dengan action *Tarpit* kita bisa mengelabui penyerang dengan tetap menerima packet data yang masuk, namun tidak dapat diakses/drop.

Firewall tarpit memiliki beberapa kelebihan dibandingkan dengan *Firewall* lainnya, yaitu:

- Mampu menunda koneksi masuk dari sumber daya penyerang sampai kelelahan dalam koneksi yang tidak berguna

- Mampu memberikan balasan *SYN/ACK* kepada paket *TCP SYN* yang masuk sehingga seolah-olah port yang discan itu terbuka, padahal sebenarnya tidak
- Mampu menolak tetapi tetap menjaga *TCP connection* yang masuk.

Dalam konteks penelitian ini, *Firewall* tarpit dipilih karena mampu mencegah serangan *Port Scanning*, *DDOS*, dan *Brute Force* pada *Router* MikroTik dengan cara menunda koneksi masuk dari sumber daya penyerang sampai kelelahan dalam koneksi yang tidak berguna. Selain itu, *Firewall* tarpit juga mampu memberikan balasan *SYN/ACK* kepada paket *TCP SYN* yang masuk sehingga seolah-olah *port* yang discan itu terbuka, padahal sebenarnya tidak. Dengan demikian, *Firewall* tarpit dapat memberikan solusi yang efektif untuk meningkatkan keamanan jaringan pada *Router* MikroTik.

Berikut beberapa *Tools* atau aplikasi yang digunakan dalam penelitian antara lain :

2.11 *Winbox*

Winbox adalah salah satu aplikasi untuk konfigurasi Mikrotik *RouterOS* menggunakan *GUI*. Aplikasi *Winbox* bisa berjalan pada *Windows* berbentuk *Portable binary*, tapi bisa juga berjalan pada *Linux* dan *MACOS* menggunakan *Wine*. Semua fungsi pada aplikasi *Winbox* hampir sama persis dengan fungsi konsol (*command line*).

2.12 *Nmap*

Salah satu *Tools* yang ada pada OS *Kali Linux* adalah *Nmap*. *Nmap* adalah sebuah aplikasi atau *Tools* yang berfungsi untuk melakukan *Port* Scanning. Aplikasi ini digunakan untuk mengaudit jaringan yang ada.

2.13 *Hydra*

Salah satu *Tools* yang ada pada *OS Kali Linux* adalah *Hydra*. *Hydra* adalah sebuah aplikasi atau *Tools* yang berfungsi untuk melakukan serangan *Brute Force* pada layanan autentikasi.

2.14 *Pentmenu*

Salah satu *Tools* yang ada pada OS *Kali Linux* adalah *Pentmenu*. *Pentmenu* adalah sebuah aplikasi atau *Tools* otomatis yang terinspirasi oleh *PentBox* yang dirancang untuk menjalankan berbagai fungsi jaringan. Alat *Pentmenu* juga melakukan pengintaian dasar seperti *Whois Records, DNS Gathering,* dll.

2.15 Metode Eksperimen

Metode eksperimen memberikan kesempatan kepada individu dan kelompok untuk secara sadar merancang dan merencanakan eksperimen untuk membuktikan kebenaran teori denganmengikuti dan menerapkan rute yang teratur dan sistematis (Rismawati, Ratman and Dewi, 2016). Penelitian eksperimen dilakukan untuk mengetahui pengaruh pemberian suatu treatment atau perlakuan terhadap subjek penelitian (Cahya, 2013).

Karakteristik dari metode eksperimen menurut (Rismawati, Ratman and Dewi, 2016) sebagai berikut :

1) Metode untuk melakukan percobaan, pengamatan dan penarikan kesimpulan terhadap sesuatu yang sedang diuji.
2) Metode yang dirancang untuk mengembangkan pengetahuan.
3) Metode yang membantu dalam pemrosesan informasi yang aktif.
4) Metode yang mengarahkan untuk mempelajari lingkungan belajar sebagai suatu teknologi
5) Metode yang digunakan untuk memecahkan masalah yang bersifat ilmiah.