BAB I
PENDAHULUAN

1.1 Latar Belakang

Jaringan Komputer adalah sekumpulan komputer yang saling terhubung melalui suatu media perantara seperti *switch*, *router*, *wireless*, kabel yang masing-masing komputer dapat bertukar informasi dan bertukar data karena berada dalam satu ruang lingkup yang disebut jaringan (Afdhol. P. Y. et al., 2023). Pesatnya perkembangan teknologi saat ini nyatanya memiliki dampak serangan terhadap jaringan pada sistem administrator. Sebagian besar jaringan komputer yang mengalami permasalahan dalam membangun sebuah jaringan komputer, hal ini dapat membuka peluang bagi para *hacker* untuk meretas dan merusak jaringan yang dibangun tersebut (Amarudin, 2018).

Sehingga bagi para pengguna teknologi yang terhubung dengan jaringan lokal maupun internet perlu waspada terhadap serangan yang dilakukan oleh pihak yang tidak bertanggung jawab. Banyak serangan-serangan yang bisa dilakukan dalam keadaan *port-port* yang terbuka diantaranya *virus, malware* dan *Trojan*. Walaupun sudah diatur dalam dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Internet dan Transaksi Elektronik (ITE) pada Pasal 30 UU ITE tahun 2008 ayat 3 yang berbunyi: “Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengaman”.

Ancaman pidana pasal 45 ayat 3 setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat 3 dipidana dengan pidana penjara paling lama 8 (delapan) atau denda paling banyak Rp 800.000.000 (delapan ratus juta rupiah) dan di dalam Kitab Undang-Undang Hukum Pidana Pasal 406 KUHP dapat di kenakan pada

kasus *deface* atau *hacking* yang membuat kerusakan atau melakukan modifikasi sistem milik orang lain. Sistem milik orang lain, yaitu :

1. Sistem *Website* atau Portal.
2. Sistem *Server*.
3. Sistem Jaringan.
4. Sistem Aplikasi.

Fokus Utama jika penyerang melakukan modifikasi atau kerusakan pada sistem jaringan khususnya pada *router mikrotik*. Keamanan jaringan *mikrotik* rentan terhadap serangan *port* yang terbuka dapat dihindari dengan menerapkan *port knocking* pada *router mikrotik*. *Simple port knocking* yang diterapkan agar sistem yang dibangun mampu mendeteksi dan menghindari serangan yang berbahaya terhadap jaringan dan langsung memberikan peringatan kepada pengelola jaringan (administrator) tentang kondisi jaringan yang sedang berjalan pada saat kejadian yang berlangsung (Saputro et al., 2020).

Port knocking merupakan suatu sistem keamanan yang bertujuan untuk membuka atau menutup akses *block* ke *port* tertentu dengan menggunakan *firewall* pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi berupa *protocol* TCP (*Transmission Control Protocol*), UDP (*User Datagram Protocol*), maupun ICMP (*Internet Control Message Protocol*). Sehingga untuk masuk dan menggunakan akses ke *port* tertentu yang telah dibatasi, maka *user* harus mengetuk terlebih dahulu dengan memasukan *rule* yang harus dilakukan terlebih dahulu. *Rule* yang hanya diketahui oleh pihak penyedia jaringan (administrator jaringan).

Sebuah sistem harus memiliki keseimbangan antar keamanan dan *fleksibilitas*. Satu cara untuk dapat mencapai sistem seperti demikian yaitu dengan mengakses *firewall*. Maka dengan menggunakan *firewall* secara tidak langsung kita dapat mendefinisikan *user* yang dapat dipercaya dan yang tidak dapat dipercaya dengan menggunakan alamat IP sebagai kriteria *filter* (Novianto et al., 2021). Hasilnya adalah sebuah sistem keamanan jaringan yang mengamankan *mikrotik* dengan metode *port knocking*. Hal ini

berfungsi sebagai alternatif untuk menjaga keamanan dalam jaringan komputer, mencegah penyerang untuk mengakses *router mikrotik* dan memungkinkan administrator untuk menentukan siapa mereka. Hanya mereka yang memiliki hak akses yang dapat masuk ke *port* tertentu (Blaise et al., 2020)

Saat ini permasalahan pada Laboratorium *High Performance Computing* (HPC) melibatkan sejumlah kendala yang signifikan dalam pengelolaan jaringan *mikrotik*. Salah satunya terkait masalah dalam pembagian *bandwith* antara dosen dan mahasiswa. Ketidakoptimalan dalam aspek keamanan jaringan *mikrotik* pada Laboratorium HPC menjadi fokus utama. Kurangnya tindakan keamanan dapat menyebabkan risiko tinggi terhadap akses yang tidak sah dan potensi ancaman keamanan yang serius. Oleh karena itu, diperlukan suatu solusi yang dapat meningkatkan keamanan jaringan pada *mikrotik* terutama ketika mengamankan *web server* yang berada di belakang NAT pada *router mikrotik* di Laboratorium HPC.

Solusi yang diusulkan melibatkan serangkaian tindakan konkret. Pertama, mengoptimalkan pembagian *bandwith* dan *hotspot user* dengan memperhatikan prioritas dan memastikan keseimbangan pembagian antara dosen dan mahasiswa. Pembuatan halaman *login page* pada perangkat *mikrotik* juga diperlukan sebagai langkah pengenalan pengguna. Tidak hanya memberikan lapisan keamanan tambahan, tetapi juga memberikan informasi yang berguna tentang pengguna. Selanjutnya yang menjadi implementasi utama untuk pengamanan jaringan pada *router mikrotik* untuk mengamankan dari potensi penyerang dan memberikan verifikasi tambahan sebelum memberikan akses ke layanan yang diinginkan pada *mikrotik* dan *mengamankan web server* yang berada pada NAT yang ada pada *mikrotik* dengan menggunakan *port knocking* dan *firewall raw* merupakan solusi yang sarankan untuk mengamankan *router mikrotik* yang berada pada Laboratorium *High Performance Computing* (HPC).

Mekanisme/skema sederhana ketika terjadi serangan pada *router mikrotik* di Laboratorium *High Performance Computing* (HPC). *Port knocking* diterapkan melalui 4 *rule* yaitu *rule* pertama lakukan *ping IP address router mikrotik* dengan *protocol* ICMP dan *rule* kedua lakukan *ping IP address router mikrotik* dengan *port telnet* dengan *protocol* TCP, *rule* ketiga lakukan hal yang sama untuk menangkap *traffic* pada *port* SSH dengan *protocol* TCP dan *rule* terakhir yaitu *droping packet* yang masuk kedalam *router* kecuali yang sudah melakukan *ping* kemudian *telnet* dan SSH seb elumnya. Rangkaian proses *knocking* harus sesuai dengan urutan *rule port knocking* yang telah dikonfigurasi, jika proses *knocking* tidak sesuai urutan maka tetap akan di *block* oleh *firewall filter* yang ada pada *router mikrotik*. Berdasarkan uraian di atas maka diperlukan pemanfaatan metode *port knocking* dalam sistem keamanan jaringan untuk mengurangi tingkat risiko, terutama pada jaringan yang ingin melakukan kejahatan dengan cara memindai *port-port* yang terbuka melalui perangkat *mikrotik* dan melakukan penyerangan *DDOS attack*.

Maka dari itu dilakukan pengujian pemanfaatan *Port knocking* yang dapat menjadi komponen penting dalam strategi mitigasi serangan DDoS, terutama ketika dihubungkan dengan perlindungan terhadap *web server* yang diamankan melalui *firewall raw* pada *mikrotik*. Dengan *port knocking*, akses *ke port-port* penting pada *router* hanya diberikan kepada pengguna yang mengikuti urutan *knocking* yang telah ditentukan, seperti mengirimkan paket ICMP, TCP Telnet, dan SSH secara berurutan. Hal ini membuat *port-port* tersebut tidak terlihat oleh penyerang yang mencoba melakukan *port scanning* atau melancarkan serangan DDoS seperti *SYN flood* dan *HTTP flood* dengan LOIC (*Low Orbit Ion Cannon*). Pada serangan *SYN flood*, di mana penyerang mencoba membanjiri *port* dengan permintaan koneksi yang tidak pernah diselesaikan, *port knocking* dapat mencegah serangan tersebut dengan menyembunyikan *port* dari akses langsung kecuali telah mengikuti urutan *knocking* yang benar. Sementara itu, untuk serangan *HTTP flood* yang berusaha membanjiri *web server* dengan permintaan HTTP palsu, *firewall raw mikrotik* dapat diatur untuk hanya menerima trafik dari klien yang telah diizinkan melalui proses *port knocking*. Maka

port knocking berfungsi sebagai gerbang pertama yang mencegah serangan DDoS menjangkau *web server*, sementara *firewall raw* menangani dan mem*filter* trafik yang masuk, memastikan hanya trafik yang sah yang dapat mencapai *web server*. Kombinasi dari *port knocking* dan *firewall raw* ini menciptakan lapisan keamanan yang kuat, mengurangi risiko kerusakan yang dapat disebabkan oleh serangan DDoS, dan menjaga ketersediaan serta kinerja *web server* di Laboratorium HPC. Solusi-solusi di atas yang telah dirancang dapat mengurangi resiko ancaman yang akan mengganggu aktivitas yang sedang berlangsung, disesuaikan dengan kondisi pada Laboratorium HPC.

1.2 Perumusan Masalah

Hasil dari permasalahan yang sudah diuraikan dari latar belakang masalah dapat di rumuskan permasalahaan yang ada pada pembuatan Metode Keamanan Jaringan *Port knocking mikrotik* pada Laboratorium *High Performance Computing* (HPC) yaitu sebagai berikut:

1. Bagaimana implementasi *port knocking* menggunakan rangkaian proses 3 ketukan yaitu *protocol* ICMP, lalu ketukan pada *port* Telnet dan *port* SSH yang ada pada *protocol* TCP dan implementasi *firewall filter* menggunakan *mikrotik RouterBoard* pada sistem keamanan jaringan Laboratorium *Performance Computing* (HPC)?
2. Bagaimana mengatur 4 baris *rule* tertentu, agar komputer yang tidak di kenali untuk mengakses ke *port* tujuan tertentu yang sedang terbuka tetapi tidak dapat masuk, tapi perangkat yang sudah dikenal dapat mengakses ke *port* tujuan dengan mengikuti 4 baris *rule* yang dibuat ?
3. Bagaimana efektivitas pengujian *port knocking* dalam meningkatkan keamanan *web server* dalam *mikrotik* menggunakan *firewall raw* dari serangan DDOS seperti SYN *flood* dan HTTP *flood*?

1.3 Batasan Masalah

Berdasarkan rumusan masalah diatas, maka batasan masalah dalam metode *port knocking* pada Laboratorium *High Performance Computing* (HPC) adalah sebagai berikut:

1. Implementasi *port knocking* menggunakan dengan rangkaian proses 3 ketukan yaitu *protocol* ICMP, lalu ketukan pada *port* Telnet dan *port* SSH yang ada pada *protocol* TCP yang hanya dibuat untuk Laboratorium *High Performance Computing* (HPC).
2. Pengguna hanya bisa mengakses *port-port* dengan *rules* yang dibuat untuk dapat mengaksesnya.
3. Pembuatan *port knocking* dengan *Mikrotik RouterBoard* RB951Ui 2nd HaP.
4. Uji coba *port knocking router mikrotik* dan keamanan *firewall filter* penelitian ini pada peran *Kali Linux* dengan melakukan *Port Scanning.*
5. Uji coba efektivitas *port knocking* pada keamanan *web server* yang di *forward* ke dalam NAT *mikrotik* dengan *firewall raw*. Penelitian ini pada peran LOIC sebagai sistem penyerang dengan jenis serangan DDOS *attack* yaitu berupa serangan SYN *flood* dan HTTP *flood*.

1.4 Tujuan Penelitian

Tujuan keamanan *port knocking* pada Laboratorium *High Performance Computing* (HPC) sebagai berikut:

1. Implementasi *port knocking mikrotik* menggunakan rangkaian proses 3 ketukan yaitu *protocol* ICMP, lalu ketukan pada *port* Telnet dan *port* SSH yang ada pada *protocol* TCP menggunakan *mikrotik RouterBoard* pada Laboratorium *High Performance Computing* (HPC) untuk meningkatkan keamanan jaringan.
2. Membuat 4 baris *rule* terhadap *router mikrotik*, agar pengguna yang tidak di kenali tidak dapat memiliki akses untuk masuk pada *port* tertentu yang

terbuka, tetapi dengan menganalisis dan di kenali oleh sistem keamanan jaringan komputer yang diberi akses oleh sistem administrator untuk perangkat yang sudah di kenali bisa dapat mengakses dengan menggunakan jaringan LAN (*Local Area Network*) ataupun internet dengan menggunakan *rule* yang dibuat.

3. Merancang dan melaksanakan pengujian dengan menggunakan *Kali Linux* dan LOIC dengan *Port Scanning* dan mitigasi serangan DDOS dengan jenis serangan SYN *flood* juga HTTP *flood* dalam meningkatkan keamanan *web server* pada *mikrotik* untuk mengukur efektivitas dan peran *port knocking* di *mikrotik*.

1.5 Manfaat Penelitian

Manfaat yang dapat diambil dari keamanan jaringan menggunakan *port knocking* pada Laboratorium *High Performance Computing* (HPC) ini yaitu sebagai berikut:

1. Dengan adanya keamanan jaringan *port knocking mikrotik* menggunakan rangkaian proses 3 ketukan yaitu *protocol* ICMP, lalu ketukan pada *port* Telnet dan *port* SSH yang ada pada *protocol* TCP untuk mengamankan jaringan komputer yang ada dan mengurangi risiko serangan akses yang tidak sah dengan menggunakan *port knocking*.
2. Bagi administrator jaringan Laboratorium *High Performance Computing* (HPC) dapat memiliki hak untuk mengakses dan memasuki *port-port* tertentu dengan mengikuti *rule* yang dibuat.
3. Mitigasi serangan DDOS dengan kombinasi *port knocking* dan *firewall raw* memberikan perlindungan berlapis terhadap serangan DDoS seperti *SYN flood* dan *HTTP flood*, memastikan bahwa hanya trafik yang sah yang dapat mencapai *web server*, sehingga menjaga stabilitas dan ketersediaan layanan.

1.6 Metode Penyelesaian Masalah

Metode Penyelesaian masalah dalam penelitian keamanan jaringan pada Laboratorium *High Performance Computing* yaitu sebagai berikut : Melakukan Identifikasi Masalah yang terjadi pada Laboratorium HPC dengan melakukan wawancara kepada Kepala Laboratorium HPC dan Laboran Laboratorium HPC dan kepada *Network Administrator* yang membangun infrastruktur jaringan komputer dan perangkat keras pada Laboratorium HPC kemudian Perancangan dan implementasi *port knocking* dan keamanan *firewall raw* pada *router mikrotik.* Dengan menggunakan *port knocking*, hanya trafik dari klien yang sah yang dapat mencapai *port-port*, sementara *firewall raw* menangani dan memblokir serangan yang lebih spesifik seperti *SYN flood* dan *HTTP flood* berdasarkan hasil wawancara maka akan melakukan analisis pada objek penelitian yang akan diteliti, dengan berdasarkan analisis yang difokuskan pada fungsi kualitas dari yang ada pada lokasi penelitian. Pada penelitian ini akan di lakukan analisis pada sistem keamanan jaringan komputer dengan menggunakan metode *port knocking*. Kemudian melakukan pengujian *Port knocking* dengan mitigasi serangan DDoS serta peran *firewall raw mikrotik* dalam melindungi *web server* dari serangan *SYN flood* dan *HTTP flood*. Berdasarkan wawancara tersebut, *port knocking* diterapkan untuk mengamankan *port-port* sensitif pada *mikrotik*, sehingga hanya pengguna yang mengikuti urutan *knocking* yang benar dapat mengakses *port* tersebut. Ini berfungsi sebagai lapisan pertama perlindungan terhadap serangan DDoS, dengan menyembunyikan *port* dari akses umum dan mengurangi kemungkinan serangan seperti *SYN flood* dan *HTTP flood* mencapai *web server*. kesimpulan, dimana pada penelitian ini hasil dicapai adalah apakah sistem jaringan di lokasi penelitian aman melalui *port* jaringan yang sudah ditentukan.