BAB I
PENDAHULUAN

1.1. Latar Belakang

Menurut Desmira D,Wiryadinata R dalam jurnalnya yang berjudul "Rancang Bangun Keamanan Port Secure Shell (SSH) Menggunakan Metode *Port Knocking*" keamanan jarinan merupakan pondasi yang sangat penting karena aspek keamanan banyak sekali yang mebutuhkannya, baik dikalangan individu maupun perusahaan. Tetapi masih banyak kalangan ataupun perusahaan yang masih menghiraukan atau kurang pedulinya dari sisi keamanan teknologi. Untuk salah satu bentuk keamanan jaringan yang sering digunakan oleh seorang administrator yaitu melakukan autentikasi login remote *Secure Shell* (SSH). Akses SSH ini berfungsi untuk meremote suatu server yang biasa digunakan untuk memantau serta mengawasi terhadap internet jaringan dan untuk memudahkan administrator untuk melakukan pengelolaan server. [1]

Menurut Mulyanto, Yudi (2022) Penyusup atau intruder sering melakukan serangan dengan serangan *brute force* terhadap sistem keamanan korban. Serangan ini berguna untuk melakukan login dengan mencoba menebak hingga berhasil untuk menemukan password yang benar sampai berhasil ditebak, entah dengan cara otomatis dengan menggunakan alat atau tools untuk membobol yaitu dengan robot (otomatis), menggunakan tools aplikasi lain ataupun secara manual. Serangan ini biasanya mengakibatkan jaringan mengalami gangguan dan perangkat yang terhubung pada jaringan didalam Mikrotik ini akan menjadi terputus tiba-tiba untuk efek dari login berulang ini adalah router bisa ridak normal jaringan pada perangkat.[2]

Menurut Jamalul'ain, Abdul (2022) Dengan menerapkan metode *Port Knocking* dan *Port Blocking* maka bisa diatur pada *firewall* yang bisa mengatur *rules* keamanan yang lebih kompleks. *firewall* akan lebih mudah dalam melakukan pengamanan yang sangat *secure* bila dimaanfaatkan dengan baik. *Firewall* bisa dirancang untuk mencegah dan menolak akses yang bisa mengancam server atau perangkat yang dimiliki. *Firewall* memiliki fungsi untuk melakukan blokir konten yang sekiranya kurang diinginkan atau kurang pantas, untuk melindungi data pribadi.[3]

1.2. Rumusan Masalah

Berdasarkan dengan latar belakang yang telah diuraikan diatas, maka dapat dibuat rumusan masalah sebagai berikut :

1. Apakah *firewall* sebagai fitur keamanan jaringan pada mikortik itu aman untuk mengatasi keamanan login SSH dari serangan *brutefoce*?.
2. Apakah metode *Port Knocking* dan *Port Blocking* dapat mengatasi serangan brutefoce yang mengancam port SSH?.

1.3. Batasan Masalah

Berdasarkan rumusan masalah yang sudah didapat maka batasan masalah yang akan digunakan sebagai pembatas ruang lingkup untuk melakukan penelitian. Maka Batasan masalah yang akan dipakai dalam penelitian ini adalah sebagai berikut :

1. Sistem dibangun dengan menggunakan *rules firewall* yang cukup kompleks.
2. Penyerangan hanya di uji coba menggunakan *brute force*.
3. Hanya membahas tentang pengomtimalan keamanan port SSH pada perangkat Mikrotik menggunakan *firewall* sebagai *rules* pengamanannya.
4. Peneliti hanya menggunakan tools Ncrack untuk uji coba serangan.
5. Hanya menggunakan perangkat Mikrotik RB951UI-2HND

1.4. Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut :

1. Mengetahui apakah *firewall* sebagai *rules* keamanan autentikasi SSH (*Scure Shell*) pada perangkat Mikrotik dapat mengatasi serangan *brute force*.
2. Mengetahui prinsip kerja metode *Port Knocking* dan *Port Blocking* apakah lebih optimal dalam penanganan serangan *brutefoce* terhadap autentikasi SSH di mikrotik

1.5. Manfaat Penelitian

Dengan dilakukannya penelitian ini maka diharapkan mendapatkan manfaat sebagai berikut :

1. Dapat memberikan rasa aman terhadap pengguna SSH, karena dalam autentikasi SSH akan semakin aman karena menggunakan *Port Knocking* dan *Port Blocking* sebagai sistem keamanan autentikasinya.
2. Manfaat bagi pengguna adalah bisa membuat orang yang menggunakan nya merasa aman saat menggunakan SSH untuk meremote suatu server atau perangkat.

1.6. Sistematika Penulisan

Pada penulisan skripsi ini mempunyai sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Bab ini merupakan pendahuluan yang menjelaskan tentang latar belakang maslaah, rumusan masalah, Batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tinjauan Pustaka, dan dasar-dasar teori yang digunakan untuk melakukan penyusunan skripsi.

BAB III METODE PENELITIAN

Bab ini didalamnya terdapat tinjauan umum tentang objek penelitian, analisis masalah, solusi yang ditawarkan, rancangan sistem keamanan, alur keamanan yang akan diterapkan

BAB IV HASIL DAN PEMBAHASAN

Bab ini merupakan tahapan saat peneliti memaparkan hasil penelitian yang telah diteliti dan di uji coba.

BAB V PENUTUP

Bab ini berisi kesimpulan dan saran yang dapat peneliti rangkum selama proses penelitian.

REFERENSI

pada halaman ini berisi jurnal dan buku yang dipakai untuk landasan penelitian ini

LAMPIRAN

Pada halaman ini berisi data konfigurasi secra detail dan menyeluruh pada implementasi penelitian ini.