

BAB I

PENDAHULUAN

A. Latar Belakang

Jaringan Komputer merupakan sekelompok komputer yang saling berhubungan antara satu dengan lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga bisa saling berbagi informasi (Pamungkas, 2016). Saat ini jaringan komputer bukan merupakan hal yang baru. Setiap instansi, telah memanfaatkan jaringan komputer. Penggunaan jaringan komputer menjadi sangat meningkat dikarenakan kebutuhan akan informasi yang menjadi semakin tinggi.

Pesatnya perkembangan jaringan ini menyebabkan individu, perusahaan, sekolah dan pemerintah bergabung dengan layanan internet, hal tersebut mengakibatkan lebih banyak pengguna ilegal menyerang serta menghancurkan jaringan dengan menggunakan situs web palsu, surat palsu, *Trojan horse*, maupun virus (Tayal et al., 2017). Target dari para pengguna ilegal atau biasa disebut *cracker* yaitu setiap orang yang sedang menggunakan internet, sehingga sekali menyusup dapat berhasil masuk ke komputer yang ditargetkan. Ketika berhasil menyusup kedalam komputer yang ditargetkan maka pengguna ilegal tersebut dapat mendapat hak akses penuh yang ada didalam komputer tersebut, dan lebih berbahaya lagi apabila terdapat dokumen yang sangat penting dan akan dimanfaatkan oleh pengguna ilegal tersebut untuk melakukan tindakan pemerasan terhadap pengguna komputer yang ditargetkan. Maka dari itu diperlukan sistem keamanan jaringan untuk meminimalisir kejahatan yang terjadi pada dunia internet.

Mikrotik merupakan sebuah Sistem Operasi Router (OS) yang digunakan untuk membuat sistem otentikasi dan penagihan. Jenis sistem ini masih digunakan untuk membuat keamanan, penagihan dan administrasi pengguna pada jaringan yang terhubung ke internet (Mukti, 2019). Penggunaan Mikrotik router seperti filtering, blokir, hotspot dan sejenisnya. Pada perkembangannya banyak sekali tipe yang dirilis oleh pihak Mikrotik salah satunya adalah Mikrotikrouterboard RB 941 *HAP Lite*.

Sebuah jaringan akan menjadi lebih aman ketika menggunakan firewall. Firewall merupakan sistem yang berguna untuk mengontrol serta menentukan paket data yang dapat masuk atau keluar dari sebuah jaringan (Gulo et al., 2021). Dengan kemampuan memonitor dan menentukan paket data maka dapat juga digunakan untuk filter data yang berguna untuk melindungi jaringan dari serangan pengguna ilegal.

Berdasarkan hasil observasi selama Asistensi Mengajar, kondisi jaringan di SMK Al-Fattah Kertosono menggunakan topologi star dimana setelah perangkat modem langsung dilalui perangkat switch. Berdasarkan hasil dari wawancara dengan Ketua jurusan Teknik Komputer dan Jaringan dari kondisi jaringan tersebut pernah mengalami kesulitan login ke perangkat Mikrotik yang diakibatkan oleh komputer yang kurang memadai serta kabel yang tidak berfungsi. Selain hal tersebut juga terjadi serangan ke jaringan sekolah menuju perangkat modem yang sering disalah gunakan untuk mengambil beberapa *bandwidth*. Dari beberapa masalah yang muncul, peneliti memutuskan untuk mengambil keamanan jaringan yang lebih penting guna mencegah terjadinya pencurian *bandwidth*.

Berdasarkan hasil tersebut maka dapat disimpulkan bahwa kondisi jaringan tersebut belum diterapkan keamanan jaringan. Peneliti mengajukan solusi yaitu setelah perangkat modem diberi router Mikrotik RB-941 yang berguna untuk mencegah penyusup masuk melalui modem karena harus melalui perangkat Mikrotik terlebih dahulu.

Untuk mengatasi masalah tersebut maka diajukannya keamanan jaringan menggunakan *firewall* berbantuan *iptables*. *Iptables* sendiri merupakan suatu solusi untuk membuat keamanan jaringan. Secara sederhana *iptables* memiliki fungsi sederhana sebagai pengatur lalu lintas data baik masuk, keluar maupun hanya sekedar lewat.

Berdasarkan pembahasan yang sudah dijelaskan sebelumnya, peneliti memutuskan untuk melakukan penelitian di SMK Al Fattah Kertosono dengan mengamankan jaringan dari serangan eksploit, *brute force* serta *DoS*. Informasi keadaan jaringan di lokasi penelitian dapat dilakukan dengan cara mengumpulkan data dan wawancara dengan pengembangan metode PPDIOO beserta untuk pengujian menggunakan *Winbox Exploit*, *Hydra* dan *Hping3*. Penelitian ini diharapkan memberi gambaran baru tentang betapa pentingnya keamanan jaringan dalam bidang pendidikan.

B. Rumusan Masalah

1. Bagaimana desain untuk keamanan jaringan guna melihat kondisi di lokasi penelitian?
2. Bagaimanakah kondisi keamanan jaringan pada perangkat Mikrotik menggunakan metode eksploit dengan *software Winbox Exploit*?

3. Bagaimanakah kondisi keamanan jaringan pada perangkat Mikrotik menggunakan metode *port knocking* dengan *software Hydra*?
4. Bagaimanakah kondisi keamanan jaringan pada perangkat Mikrotik menggunakan metode *filter packet* dengan *software Hping3*?

C. Tujuan Penelitian Pengembangan

1. Mengembangkan desain untuk keamanan di lokasi penelitian.
2. Melakukan pengujian keamanan jaringan pada perangkat Mikrotik menggunakan *software Winbox Exploit*.
3. Melakukan pengujian keamanan jaringan pada perangkat Mikrotik menggunakan metode *port knocking* dengan *software Hydra*.
4. Melakukan pengujian keamanan jaringan pada perangkat Mikrotik menggunakan metode *Filter packet* dengan *software Hping3*.

D. Spesifikasi Produk yang diharapkan

Spesifikasi produk yang diharapkan dalam penelitian ini adalah sebagai berikut:

1. Router Mikrotik merupakan sebuah perangkat keras yang berguna untuk menghubungkan antar jaringan, manajemen *bandwidth*, memonitoring paket data dan memblokir sebuah situs. Didalam Mikrotik inilah konfigurasi *port knocking* dilaksanakan.
2. Komputer/Laptop adalah sebuah perangkat yang akan digunakan sebagai *client* yang digunakan untuk konfigurasi router.

3. Kabel UTP dan Konektor RJ-45 adalah sebuah kabel yang dibagian kedua ujungnya diberikan sebuah konektor RJ-45 yang digunakan untuk menghubungkan sebuah perangkat komputer/laptop
4. *Software Winbox* adalah sebuah perangkat lunak yang memudahkan pengguna menadministrasi didalam router khususnya dengan merek Mikrotik
5. *Software Nmap* adalah sebuah alat yang digunakan untuk mencari celah pada sebuah jaringan khususnya celah pada sebuah *port* pada jaringan tersebut.
6. *Software Hydra, Winbox Exploit dan Hping3* adalah sebuah alat yang akan peneliti manfaatkan untuk menguji keamanan jaringan yang pada jaringan tersebut.
7. *Software Virtual Box* adalah sebagai alat untuk membuat virtualisasi didalam sebuah komputer, disini akan peneliti gunakan untuk diisikan operasi sistem Linux dengan distro *Backbox*.
8. *ISO Backbox Linux* adalah sebuah file iso yang akan digunakan untuk menginstal *Backbox Linux* di *Virtual Box*

E. Batasan Penelitian Pengembangan

Batasan yang dibuat oleh pengembang penelitian ini antara lain sebagai berikut:

1. Melakukan wawancara tentang kondisi keamanan jaringan jaringan di lokasi penelitian.
2. Melakukan serangan menggunakan *software Winbox Exploit, Hydra, serta Hping3*.
3. Mengkonfigurasi keamanan jaringan yang berada pada lokasi penelitian dari serangan dari luar.

4. Menguji keberhasilan hasil konfigurasi dengan menggunakan *software Winbox Exploit, Hydra, serta Hping3*.

F. Pentingnya Penelitian Pengembangan

Penelitian ini perlu dilakukan dikarenakan di lokasi penelitian sering terjadi pencurian *bandwidth* pada modem. Dengan menambahkan Routerboard Mikrotik RB 941 setelah perangkat modem serta menerapkan keamanan jaringan dengan metode *Port Knocking* serta *Filter Packet Raw* dapat digunakan untuk mencegah pengguna illegal mencoba menyusup ke perangkat modem serta router.

G. Definisi Istilah

1. *Port Knocking* adalah sebuah konsep yang menyembunyikan layanan jarak jauh di dalam firewall sehingga memungkinkan port tersebut diakses hanya untuk menemukan service setelah klien berhasil mengautentikasi ke firewall. Hal tersebut dapat membantu menangkal pemindai mengetahui service apa yang saat ini tersedia di firewall dan juga berperan sebagai pertahanan terhadap serangan zero-day (Sel et al., 2016).
2. Keamanan jaringan adalah sebuah sistem yang terhubung dengan jaringan yang digunakan sebagai pelindung untuk mencegah serangan dari pihak luar.
3. Mikrotik adalah sistem operasi khusus komputer berbasis Linux yang berdiri sendiri dan berfungsi sebagai router. Mikrotik dirancang agar mudah digunakan dan digunakan dengan sangat baik untuk keperluan administrasi jaringan komputer, seperti merancang dan membangun jaringan komputer (Riadi, 2011).

4. *Firewall* adalah sistem atau perangkat yang memungkinkan lewatnya lalu lintas jaringan yang dianggap aman dan mencegah lalu lintas jaringan yang tidak aman. *Firewall* umumnya digunakan untuk mengontrol akses ke siapapun yang memiliki akses ke jaringan pribadi terhadap pihak ketiga atau pencuri data lainnya.
5. *Brute force* adalah algoritma yang memecahkan masalah kode dengan cara yang sangat sederhana, lugas dan jelas. Memecahkan masalah pemecahan kode menggunakan algoritma *brute force* akan menemukan serta mencari semua kode yang mungkin dengan karakter input dan panjang kode tertentu, jelas dengan banyak kombinasi kode. (Gunawan, 2016).
6. *Hydra* adalah sebuah perangkat lunak yang berisikan beberapa alat yang salah satunya *brute force* yang akan digunakan untuk pengujian penelitian ini.
7. *Hardware* adalah sebuah perangkat komputer yang terdiri dari susunan komponen elektronika dalam bentuk fisik (berupa benda) dan memiliki peran tertentu (Putri et al., 2015).