BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan jamandari hari kehari semakin meningkat, dimana para ahli mengembangkan ilmu pengetahuannya baik dalam bidang industri, kesehatan, keamanan jaringan dan lainnya. Semakin meluasnya perkembangan pembangunan terhadap teknologi semakin banyak juga pihak-pihak yang tidak berwenang melakukan peretasan sehingga rentan terjadinya penyusupan, oleh sebab itu maka aplikasi yang digunakan oleh pengguna yang terhubung secara langsung dengan internet harus mewaspadain terjadinya penyusupan oleh pihak yang tidak berwenang, karena pada saat sekarang ada banyak pengguna internet menjadi korban penyusupan. Salah satu penyusupan yang saat ini berhasil di retas dan sering dilakukan adalah situs *UML, Malwere, Trojan, Virus,* dan pemindaian *port*. Menggunakan jaringan, pemindaian *port* adalah sebuah metode untuk menemukan *port* komputer yang terbuka.

PT Air Batam Hulu adalah sebuah perusahaan yang beralamat Gedung A-WTP Moya Muka Kuning Jl.Letjend Supranto merupakan perusahaan air dibatam yang menjaga keamanan pengelolahan air minum. Namun pada sistem yang digunakan oleh perusahaan masih terdapat Pihak-pihak yang tidak berwenang melakukan peretasan sehingga rentan terjadinya penyusupan terhadapa keamanan data, selain itu dalam suatu sistem jaringan komputer terdapat bentuk ancaman baik

dari segi fisik ,maupun logika seperti *Sniffer, Spoofing, Preaking, Remote Attack, Hole, Hacker, Craker* dan lainnya, Salah satu penyusupan yang saat ini berhasil di retas dan sering dilakukan adalah situs *UML, Malwere, Trojan, Virus,* dan pemindaian *port.*

Jaringan komputer adalah sekumpulan terminal komunikasi atau perangkat yang saling terhubung dengan tujuan memungkinkan berbagi informasi dan data secara efisien. Jaringan komputer memungkinkan komputer-komputer client untuk berkomunikasi, berbagi sumber daya, dan mengakses data dari server. Namun, bersama dengan manfaatnya, jaringan komputer juga menghadapi berbagai ancaman keamanan. Beberapa bentuk kerawanan pada jarinngan yang umum termasuk:, Spoofing, Preaking, Remote Attack, Hole, Hacker, Craker dan lainnya (Amien et al., 2020).

Security jaringan komputer memiliki kaitannya atas kerawanan data, karena itu kerawanan jaringan memiliki peran berharga dalam lindungi data sama sekali tiada memiliki wewenang. Serbuan bisa bertujukan kepada intansi,perusahaan atau lembaga tertentu. Penyusupan terhadap data dilakukan dengan melihat celah-celah pada jaringan komputerdan salah satunya melalui *port-port*. Untuk mengatasi serangan pada *port* itbuatlah langkah yang sesuai dengan security keamanan yaitu *port knocking. Port Knocking* adalah bentuk sistem *security* guna untuk menjaga jaringan dengan cara menutup akses *port* yang tidak memiliki hak untuk dapat megakses nya (Riska et al., 2018).

Port Knocking yakni metode keselamatan yang menggunakan firewall agar berfungsi buka dan tutup akses ke port yang digunakan untuk pengguna tertentu.

dengan mengirimkan paket atau koneksi tertentu dalam urutan yang telah ditentukan sebelumnya. Metode ini memungkinkan akses ke port-port yang sebelumnya diblokir hanya jika pola koneksi yang benar terdeteksi. *Port Knocking* memanfaatkan protokol TCP, UDP, atau ICMP untuk mengirimkan paket-paket tersembunyi dalam pola tertentu, sehingga firewall dapat mendeteksi dan meresponsnya dengan membuka jalan masuk pada port tersebut sesuai dengan aturan telah ditentukan. Sebab itu untuk dapat mengakses dan menggunakan port yang telah dibatasin pengguna diharuskan untuk mengetuk dan memasukan aturan yang harus dilakukan terdahulu. Aturan dibuat untuk hanya diketahui oleh *adimistrator* atau penyedia layanan. Sistem yang baik adalah sistem yang mempunyai tingkat seimbang antar *security* dengan fleksibelitas dengan melakukan hal yaitu pemakaian *firewall* dengan alat IP sebagai kriteria filter, maka dengan menggunakan tersebut dapat membedakan pengguna yang bisa diberikan kepercayaan dan yang tidak bisa (Sembiring et al., n.d.)

Konfigurasi routing pada *Router* dapat memakai statistik dan dinamis *routing* untuk mengatur raouting. Statistik tidak membutuhkan sumber daya sehingga dapat dipergunakan untuk jaringan komputer yang tidak terlalu besar. Namun statik *routing* akan sulit untuk admin dalam menjaga dan mengatur *konfogurasi table routing* sehingga dapat tetap digunakan jika pada jaringan yang lebih besar. Karena itu, *routing* dinamis sebagai pelengkap proses *routing* jaringan dengan otomatis,.

Proses dari isi data pada *routing table* dilakukan dengan otomatis dikenal sebagai *routing* dinamis. Dynamic *routing* diperlukan dalam kasus dimana ada pemakaian aturan lebih yang mungkin untuk pencapaian yang sama pada jaringan.

Protokol *routing* menata *router-router* untuk bisa melakukan komunikasi sama lainnya dan membagikan fakta *routing* yang dapat membarui isi *forwarding table* pada situasi jaringan yang dapat memungkinkan *router* untuk melihat situasi jaringan mana paling akhir dan melanjutkan data ke arah yang lebih tepat.

Berlandaskan uraian yang terdapat di atas maka peneliti mengambil judul penelitian ”**IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN *PORT KNOCKING***

1.2 Identifikasi Masalah

Dari penyampaian latar belakang maka dapat diidentifikasi sebagai berikut:

1. Pihak-pihak yang tidak berwenang melakukan peretasan sehingga rentan terjadinya penyusupan terhadapa keamanan data.
2. Dalam suatu sistem jaringan komputer terdapat bentuk-bentuk ancaman baik dari segi fisik ,maupun logika seperti *Sniffer, Spoofing, Preaking, Remote Attack, Hole, Hacker, Craker* dan lainnya
3. Salah satu penyusupan yang saat ini berhasil di retas dan sering dilakukan adalah situs *UML, Malwere, Trojan, Virus,* dan pemindaian *port.*

1.3 Batasan Masalah

Adapun batasan pada permasalahan penelitian ini yaitu:

1. Hanya mengimplementasikan *Knocking port* pada *Board Router Mikrotik*
2. Menggunakan alat pendukung yaitu 1 laptop untuk membuatnya.
3. Pengecekan soket port dilakukan dengan menggunakan aplikasi PuTTY.

1.4 Rumusan Masalah

Dari uraian yang ada pada penelitian, maka di bawah ini adalah rumusan masalah:

1. Bagaimana cara peningkatan keamanan jaringan komputer dengan metode *port knock?*
2. Bagaimana cara mengetikkan *port knock* pada *Router Board Mikrotik??*
3. Bagaimana cara administrator jaringan memantau jaringan?

1.5 Tujuan Penelitian

Tujuan penelitian yang akandi capai oleh peneliti yaitu:

1. Meningkatkan keamanan jaringan komputer
2. Untuk mengurangi terjadinya serangan terhadap komputer
3. Mencegah dan mengidentifikasi pengguna yang tidak berwenang di komputer.

1.6 Manfaat Penelitian

Dibedakan atas dua golongan manfaat penelitian yaitu:

1.6.1 Manfaat Teoritis

1. Bagi Peneliti

   Sebagai ilmu pengetahuan baru tentang cara implemetasi *security* jaringan mempergunakan *port Knocking*

2. Bagi Pembaca

   Sebagai masukan kepada pembaca agar mengetahui dalam keamanan *Router OS Mikrotik* serta monitoring jaringan.

3. Bagi Akademisi

   Sebagai refernsi tambahan bagi peneliti selanjutnya tentang keamanan jaringan

1.6.2 Manfaat Praktis

1. Untuk dapat membantu mengamankan jaringan komputer
2. Untuk memudahkan banyak organisasi saling bertukar informasi tanpa perlu khawatir tanpa ada gangguan dari serangan *cracker*