

BAB I

PENDAHULUAN

A. Latar belakang

Keamanan jaringan adalah konsep untuk mencegah pengguna yang tidak sah masuk kedalam sistem jaringan komputer. Sistem harus tetap dilindungi dari segala macam serangan dan usaha penyusupan atau pemindaian oleh pihak yang tidak memiliki hak. Langkah-langkah pencegahan dapat membantu administrator untuk menghentikan pengguna yang tidak sah untuk mengakses sistem jaringan komputer. Keamanan jaringan komputer berfungsi untuk mengantisipasi resiko-resiko yang akan terjadi pada jaringan komputer yang dapat mengganggu aktivitas yang sedang terjadi pada sistem jaringan komputer . Ada tiga hal dalam konsep keamanan jaringan, yaitu ingkat bahaya, ancaman dan kerapuhan sistem. Menurut John D. Howard berpendapat dalam bukunya yang berjudul “*An Analysis of security incidents on the internet*” bahwa: “Keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab” (Purba & Efendi, 2021).

Keamanan jaringan komputer sangat penting untuk mengontrol akses jaringan dan mencegah akses tidak sah ke sumber daya jaringan. Tugas keamanan jaringan dikendalikan oleh administrator jaringan. Mengenai keamanan, ada lima poin yang didefinisikan. Artinya kerahasiaan, informasi (informasi) yang diperlukan hanya tersedia bagi orang yang berwenang, integritas, informasi yang diperlukan hanya dapat diubah oleh orang yang

berwenang, ketersediaan, informasi yang diperlukan tersedia peserta memiliki otorisasi, otentikasi, identifikasi yang benar dari pengirim informasi, jika diperlukan, memastikan bahwa kode pribadi yang diterima tidak palsu, tidak ada penolakan, pengirim informasi menerima pesan yang meminta agar penerima juga tidak dapat menolak kiriman. Santoso, Ainurohman (2022).

Di era saat ini perkembangan jaringan komputer sangat pesat, karena akses terhadap internet sangat dibutuhkan oleh semua kalangan sekarang ini. Internet tidak hanya di akses untuk mencari informasi bagi orang – orang yang membutuhkannya, tetapi juga di akses oleh *hacker*. Dengan tujuan tertentu mereka melakukan penyusupan yang bisa merugikan para pemilik server dan jaringan komputer. Mereka menggunakan berbagai macam serangan jaringan komputer dengan tools yang dibuat secara mandiri ataupun yang telah ada. Kecanggihan serangan dan tools pada jaringan komputer berbanding terbalik dengan pengetahuan tentang penyusupan pada jaringan komputer.

Tujuan dari keamanan jaringan komputer adalah untuk mengantisipasi resiko pada jaringan komputer berupa bentuk ancaman fisik maupun logik baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer. Selain itu, untuk menjaga data pada sistem komputer agar aman dari berbagai (Akbar et al., 2021)

Peran jaringan komputer juga sangat diperlukan untuk mengintegrasikan data antar beberapa komputer yang saling terhubung sehingga memperoleh suatu data yang relevan. Karena itulah pentingnya

kemanan jaringan agar pengguna jaringan komputer tidak menyalahgunakan manfaat dari suatu jaringan komputer. Namun ada beberapa pihak yang tidak bertanggung jawab yang sering mencoba menyalah gunakan manfaat ini salah satunya yaitu membuka situs hiburan pada waktu jam kerja sedang berlangsung yang dapat mengurangi produktifitas guru dalam melakukan pekerjaanya (Teknologi & Bisnis, 2022).

Jaringan komputer terdiri dari komputer, *software*, dan perangkat jaringan yang bekerja bersama dalam satu ruang lingkup yang disebut jaringan. Jaringan komputer telah menjadi suatu hal penting dalam dunia pendidikan. Banyak sekolah yang menggunakan jaringan komputer untuk membantu kegiatan belajar mengajar. Infrastruktur jaringan komputer merupakan hal yang cukup penting sehingga perlu diperhatikan dan dikelola dengan baik agar kinerja jaringan dapat tetap maksimal (Lestari & Permana, 2019).

Penggunaan jaringan komputer selain di perkantoran juga digunakan di sekolah, utamanya yang berorientasi pada kejuruan, dimana didalamnya terdapat laboratorium komputer seperti halnya pada SMK Negeri 1 Kelam Permai. Gambaran laboratorium SMK Negeri 1 Kelam Permai gunakan sebagai penunjang dalam kegiatan belajar mengajar, salah satunya adalah laboratorium komputer sebagai sarana penunjang dalam pembelajaran. Laboratorium komputer berfungsi sebagai pusat teknologi informasi dan komunikasi (TIK) yang menunjang iklim belajar di

lingkungan sekolah sehingga dapat meningkatkan minat siswa dalam peningkatan prestasi belajar demi terciptanya sumber daya manusia yang terampil, berwawasan luas, dan disiplin. Laboratorium komputer merupakan sebuah ruangan yang disediakan sekolah untuk menunjang berbagai kegiatan pembelajaran yang membutuhkan komputer dan juga jaringan internet. Pada ruangan ini, terdapat berbagai fasilitas seperti komputer, infocus, meja, kursi, dan lainnya. Kegiatan yang bisa dilakukan di laboratorium ini antara lain adalah pembelajaran dengan menggunakan komputer. Selain itu, laboratorium komputer juga dapat digunakan untuk berbagai mata pelajaran yang membutuhkan fasilitas komputer untuk menunjang agar kegiatan belajar mengajar dapat terlaksana dengan baik dan juga dapat digunakan untuk melakukan ujian secara *online*.

Studi tentang jaringan komputer akan membantu siswa SMK memahami bagaimana suatu jaringan terdiri dari setiap komputer, yang akan membentuk jaringan lokal atau global dari perangkat tersebut. Namun, pembelajaran jaringan komputer masih dianggap kurang menarik oleh siswa. Tidak ada perangkat pembelajaran yang inovatif dan terintegrasi dengan materi pembelajaran jaringan komputer. Hal ini menyebabkan pendidik kesulitan dalam memberikan pembelajaran yang menarik dan efektif. Maka dari itu di perlukannya sistem *port knocking* yang bertujuan untuk membuka atau menutup akses *block*. (Cahyaningrum & Cuhazriansyah, 2023).

Port knocking adalah metode yang digunakan untuk membuka akses ke port tertentu yang telah diblokir oleh *Firewall* pada perangkat jaringan dengan mengirimkan paket atau koneksi tertentu, Kelebihan port knocking dengan *firewall* adalah walaupun semua port tertutup, mereka memiliki hak akses dan mengetahui *knocking* untuk membuka *port* sehingga *user* dapat selalu menggunakan *port* yang telah dibuka (Santoso, Affandi, et al., 2022).

Port knocking adalah metode keamanan yang digunakan untuk mengamankan akses ke layanan jaringan seperti SSH atau web server (Novianto et al., 2021). Pada dasarnya cara kerja dari *port knocking* adalah menutup semua *port* yang ada, dan hanya *user* tertentu saja yang dapat mengakses sebuah *port* yang telah ditentukan, yaitu dengan cara mengetuk terlebih dahulu (Yudi Mulyanto et al., 2021)

Maka dari itu tujuan *port knocking* di laboratorium, seperti halnya di lingkungan jaringan yang lebih luas, adalah untuk meningkatkan keamanan jaringan dengan cara menyembunyikan atau mengaburkan port yang terbuka. *Port knocking* adalah teknik keamanan di mana akses ke layanan jaringan (seperti SSH atau web *server*) diaktifkan oleh urutan akses ke port tertentu dalam urutan yang telah ditentukan sebelumnya. (Yudi Mulyanto et al., 2021).

Dalam konteks laboratorium, *port knocking* dapat digunakan untuk melatih praktik keamanan jaringan dan membiasakan siswa dengan konsep-konsep seperti pengaburan port dan akses terenkripsi. Ini dapat

membantu mereka memahami bagaimana mengatur lapisan keamanan tambahan di atas layanan jaringan dasar, serta memahami konsep akses jarak jauh yang aman (Yudi Mulyanto et al., 2021).

Di samping itu, menggunakan *port knocking* di laboratorium dapat membantu siswa memahami cara mengonfigurasi dan mengelola alat-alat keamanan seperti *firewall* untuk memperkuat keamanan jaringan. Hal ini bisa menjadi bagian dari latihan yang lebih luas dalam pengujian penetrasi atau pengelolaan keamanan jaringan (Riska et al., 2019). Lebih lanjut dijelaskan oleh Riska bahwa dari itu cara *kerja port knocking* adalah menutup semua port yang ada, dan hanya user tertentu saja yang dapat mengakses sebuah port yang telah ditentukan, yaitu dengan cara mengetuk terlebih dahulu.

Berdasarkan hasil pra observasi yang dilakukan oleh peneliti terungkap bahwa Keamanan jaringan komputer di SMK Negeri 1 Kelam Permai masih belum aman, maka dari itu SMK Negeri 1 Kelam Permai sudah menggunakan keamanan jaringan komputer menggunakan *port knocking* agar bisa mengamankan sistem jaringan sehingga tidak terjadi serangan atau gangguan dari luar jaringan komputer. Maka alasan peneliti ingin meneliti judul tersebut karena belum pernah ada yang menganalisis keamanan jaringan menggunakan *port knocking* di laboratorium SMK Negeri 1 Kelam Permai.

Dari latar belakang tersebut di atas, peneliti tertarik untuk melakukan penelitian tentang keamanan jaringan komputer menggunakan

port knocking pada laboratorium komputer SMK Negeri 1 Kelam Permai dengan Judul “Analisis Keamanan Jaringan Komputer Menggunakan *Port Knocking* Pada Laboratorium komputer SMK Negeri 1 Kelam Permai.

B. Rumusan Masalah

Berdasarkan pemaparan latar belakang diatas, agar mempermudah penelitian menganalisis keamanan jaringan komputer Menggunakan Port Knocking pada laboratorium komputer SMK Negeri 1 Kelam., maka dapat dirumuskan sub-sub masalah sebagai berikut:

1. Bagaimana menganalisis keamanan jaringan komputer menggunakan *port knocking* pada laboratorium komputer SMK Negeri 1 Kelam Permai?
2. Bagaimana penerapan *port knocking* sebagai metode keamanan jaringan komputer pada laboratorium komputer SMK Negeri 1 Kelam Permai
3. Bagaimana keamanan jaringan pada laboratorium komputer SMK Negeri 1 Kelam Permai?

C. Tujuan penelitian

Adapun tujuan penelitian berdasarkan sub-sub masalah di atas, adalah sebagai berikut:

1. Untuk mengetahui keamanan jaringan komputer menggunakan *port knocking* pada laboratorium komputer SMK Negeri 1 Kelam Permai.
2. Untuk mengetahui penerapan *port knocking* sebagai metode keamanan jaringan komputer pada laboratorium komputer SMK Negeri 1 Kelam Permai.

3. Untuk mengetahui keamanan jaringan komputer pada laboratorium komputer SMK Negeri 1 Kalam Permai

D. Manfaat Penelitian

Manfaat penelitian terbagi menjadi dua, yaitu manfaat yang bersifat teoritis dan manfaat yang bersifat praktis.

1. Manfaat Teoritis

Secara teoritis penelitian ini bermanfaat untuk mengetahui cara Menerapkan konsep keamanan jaringan dalam membantu melindungi data sensitif yang dimiliki oleh sekolah, seperti data pribadi siswa, catatan akademis, dan informasi administratif.

2. Manfaat Praktis

a. Bagi guru,

Hasil penelitian ini diharapkan mampu meningkatkan kualitas keaman jaringan komputer dalam konteks Sekolah Menengah Kejuruan.

b. Bagi Siswa

Memahami keamanan jaringan juga dapat merangsang inovasi dan kreativitas siswa dalam menciptakan solusi keamanan yang efektif dan efisien.

c. Bagi Sekolah

Mampu memberikan rekomendasi agar tetap menjaga dan meningkatkan keamanan jaringan.

d. Bagi Peneliti

Penelitian ini diharapkan dapat memberikan wawasan serta meningkatkan pengetahuan peneliti tentang keamanan jaringan komputer dalam konteks Sekolah Menengah Kejuruan.

e. Bagi Peneliti Selanjutnya

Penelitian ini sebagai dasar untuk penelitian lain dalam mengembangkan kompetensi serta mengembangkan produk media pembelajaran dengan tema keamanan jaringan komputer dalam konteks Sekolah Menengah Kejuruan.

f. Bagi lembaga STKIP Persada Khatulistiwa Sintang

Hasil penelitian dapat dijadikan sebagai sumber ilmu dan untuk menambah wawasan tentang keamanan jaringan komputer dan konteks Sekolah Menengah Kejuruan.

E. Definisi Istilah

Peneliti menjelaskan beberapa definisi istilah, dalam penelitian ini untuk menghindari terjadinya kesalahpahaman dalam memahami judul penelitian, di definisi istilah ini peneliti hanya ingin menganalisis dan mendiskripsikan bagaimana keamanan jaringan komputer. Adapun definisi dalam penelitian sebagai berikut:

1. Keamanan jaringan Komputer

Keamanan jaringan adalah konsep untuk mencegah pengguna yang tidak sah masuk kedalam sistem jaringan komputer. Sistem harus tetap dilindungi dari segala macam serangan dan usaha penyusupan atau

pemindaian oleh pihak yang tidak memiliki hak. Langkah-langkah pencegahan dapat membantu administrator untuk menghentikan pengguna yang tidak sah untuk mengakses sistem jaringan komputer. Keamanan jaringan komputer berfungsi untuk mengantisipasi resiko-resiko yang akan terjadi pada jaringan komputer yang dapat mengganggu aktivitas yang sedang terjadi pada sistem jaringan komputer. Ada tiga hal dalam konsep keamanan jaringan, yaitu ingkat bahaya, ancaman dan kerapuhan sistem.

2. *Port Knocking*

Port knocking adalah sebuah mekanisme keamanan yang bertujuan untuk mengontrol akses ke *port* tertentu dengan menggunakan *firewall* pada perangkat jaringan. Caranya adalah dengan mengirimkan paket atau koneksi tertentu dalam bentuk protokol TCP (*Transmission Control Protocol*) UDP (*User Datagram Protocol*), maupun ICMP (*Internet Control Message Protocol*). (Keamanan & Menggunakan, 2023).

Konfigurasi *port knocking* adalah teknik keamanan yang digunakan untuk menyembunyikan layanan jaringan yang berjalan di sebuah mesin. Cara kerjanya adalah dengan mengizinkan akses ke layanan tersebut hanya setelah serangkaian permintaan koneksi yang tepat ke *port-port* tertentu dilakukan dalam urutan yang benar.