BAB I
PENDAHULUAN

1.1. Latar Belakang

Kebocoran data pribadi, khususnya data kependudukan yang sangat vital, adalah masalah serius yang kerap terjadi di Indonesia. Kebocoran ini melibatkan berbagai informasi pribadi yang dapat dimanfaatkan untuk beragam tujuan, termasuk validasi transaksi finansial dan tindakan ilegal. Sebagai contoh, terjadi kebocoran data kependudukan melalui server BPJS dengan jumlah mencapai 279 juta, memungkinkan akses ilegal ke informasi seperti nama, tanggal lahir, dan nomor KTP. Situasi ini berpotensi disalahgunakan untuk kegiatan seperti penggantian kartu SIM dan pendaftaran kredit online, yang menimbulkan risiko keamanan besar bagi individu yang data mereka bocor. Oleh karena itu, perlindungan data pribadi sangat penting dan memerlukan tindakan cepat serta efektif dari pemerintah, pengelola data kependudukan, dan pihak terkait untuk menghindari dampak lebih parah terhadap masyarakat. (Sutrisna, 2021).

Selain dalam sektor pemerintahan dan kesehatan, kebocoran data bisa juga terjadi dalam sektor pendidikan, khususnya universitas. Universitas Z merupakan salah satu universitas yang berlokasi di Surabaya, Jawa Timur. Universitas Z telah lama menggunakan sistem X serta sistem Y untuk menunjang kegiatan belajar-mengajar yang berlangsung pada lingkungan universitas. Pada tahun 2022, beberapa situs yang dimiliki oleh Universitas Z diretas oleh sekelompok peretas. Peretasan ini dilakukan dengan melakukan perubahan wajah (*deface*) situs yang ada pada beberapa situs yang dimiliki Universitas Z. Meski tidak ada berita berapa data yang berhasil dicuri atau diambil pada peristiwa ini, hal tersebut menandakan bahwa situs-situs yang ada pada Universitas Z masih memiliki kerentanan sehingga keamanan yang dimiliki Universitas Z masih perlu ditingkatkan lagi. Penelitian yang dilakukan oleh Fernanda Tinambunan pada sistem X dengan menggunakan OWASP TOP 10 mengungkapkan bahwa pada sistem X memiliki beberapa celah keamanan dengan satu celah keamanan tingkat tinggi yang perlu diperhatikan. Dengan dua informasi yang didapat, maka perlu juga dilakukan pengujian keamanan jaringan yang dimiliki oleh Universitas Z agar data-data

penting yang ada pada Universitas Z semakin terjaga dengan baik.

Keamanan jaringan atau sistem informasi adalah kumpulan kebijakan dan praktik yang diterapkan untuk menanggulangi risiko akses ilegal, perubahan sistem, penyalahgunaan, atau serangan *denial-of-service* terhadap jaringan komputer dan sumber daya yang tersedia. Penerapan teknologi keamanan adalah langkah penting dalam melindungi aset informasi dari berbagai ancaman. Teknologi ini termasuk sistem seperti *firewall*, enkripsi, deteksi intrusi (IDS), SSL (*Secure Sockets Layer*), *antivirus*, *IPSec* (*Internet Protocol Security*), autentikasi, dan teknologi lain yang dirancang untuk memperkuat keamanan dan integritas data (Bustami & Bahri, 2020).

Firewall merupakan sistem keamanan yang bertugas mengawasi dan mengatur lalu lintas data pada jaringan. Tujuannya adalah untuk memutuskan apakah suatu paket data dapat diterima atau harus diblokir sesuai dengan aturan yang sudah ditentukan. Melalui teknik penyaringan, *firewall* dapat mengenali dan menolak konten atau paket data yang dianggap ilegal, tidak sesuai, atau tidak berizin, mencegahnya dari memasuki jaringan. Penerapan aturan yang akurat dalam *firewall* memungkinkan administrator jaringan untuk mengendalikan lalu lintas dan *bandwidth* secara efisien, serta menangani isu penyebaran *malware* yang bisa merusak atau menghambat performa jaringan (Putra et al., 2023).

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan di atas, maka didapatkan perumusan masalah penelitian sebagai berikut :

1. Bagaimana cara percobaan penetrasi pada pengujian keamanan *firewall* sistem X dan sistem Y di Universitas Z?
2. Dengan menggunakan percobaan penetrasi sebagai metode pengujian, seberapa aman keamanan *firewall* yang digunakan pada sistem X dan sistem Y di Universitas Z?

1.3. Tujuan

Dengan rumusan masalah yang sudah dijabarkan di atas, maka didapatkan tujuan penelitian ini sebagai berikut:

1. Mempelajari cara penerapan percobaan penetrasi untuk menguji keamanan *firewall* sistem X dan sistem Y di Universitas Z.
2. Mengetahui tingkat keamanan *firewall* sistem X dan sistem Y di Universitas Z setelah dilakukan percobaan penetrasi.

1.4. Manfaat

Dengan rumusan masalah dan tujuan penelitian yang sudah dijabarkan di atas, maka diharapkan adanya manfaat dalam penelitian ini, diantaranya:

1. Manfaat Bagi Peneliti

   Manfaat yang didapatkan oleh peneliti adalah dapat mengetahui bagaimana cara kerja percobaan penetrasi sebagai alat untuk menguji keamanan *firewall* pada suatu sistem instansi yang dapat digunakan sebagai bekal untuk prospek kerja ke depannya.

2. Manfaat Bagi Instansi

   Manfaat yang didapatkan oleh instansi dalam hal ini adalah Universitas Z adalah dapat mengetahui seberapa rentan *firewall* sistem X dan sistem Y mereka sehingga dapat dilakukan pembaharuan sistem *firewall* untuk meningkatkan keamanan jaringan yang dimiliki agar dapat melindungi data-data vital yang ada di dalamnya.

1.5. Batasan Masalah

Adapun batasan-batasan masalah yang diterapkan untuk menunjang penelitian ini agar dapat semakin fokus kepada topik dan permasalahan yang ingin diangkat, diantaranya:

1. Ruang lingkup penelitian ini hanya berfokus pada *firewall* sistem yang ada pada Universitas Z.
2. Sistem yang akan diuji keamanan jaringan *firewall*nya adalah sistem X serta sistem Y Universitas Z.
3. Pengujian hanya dilakukan sampai penemuan kerentanan yang ada pada sistem serta pemberian solusi yang dapat diberikan, penerapan solusi hanya dilakukan pada satu kerentanan dengan penerapan secara teori.

4. Pengujian dilakukan secara eksternal, sehingga terdapat beberapa informasi yang tidak dapat diambil pada saat pengujian.