BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Berdasarkan data pelaporan kejahatan siber di Indonesia tahun 2019 – 2020 Februari tercatat lebih dari 2000 kasus yang dikutip dari lokadata.beritagar.id. Penyebaran konten provokatif sebanyak 1769 kasus pelaporan, penipuan *online* sebanyak 1617 kasus pelaporan, pornografi sebanyak 364, dan pencurian data sebanyak 143 kasus pelaporan tentu hal ini dipengaruhi oleh perkembangan teknologi dan informasi yang begitu cepat. Perkembangan teknologi dan informasi sangatlah cepat, mulai dari proses pembuatan teknologi itu sendiri hingga proses pertukaran informasi di berbagai media *online*. Hal ini dipicu oleh ketatnya persaingan antara individu atau kelompok yang terus menciptakan inovasi pada bidang teknologi dan informasi. BYOD *(Bring Your Own Device)*, istilah ini muncul 10 tahun yang lalu menggambarkan tentang kondisi dimana setiap orang bisa mengerjakan sesuatu tanpa terhalang oleh jarak dan waktu karena teknologi yang semakin hari semakin canggih sehingga dapat dibawa kemana saja [1]. Dengan internet semua akses informasi bisa diakses dengan mudah, dimana dan kapan saja. Hal tersebut menimbulkan kekhawatiran bagi para pakar kemanan teknologi dan informasi, pasalnya ketika semua orang dapat mengakses informasi dengan sangat mudah, disaat yang bersamaan tidak sedikit pelaku kejahatan memanfaatkan situasi ini untuk mendapatkan informasi penting dari pengguna yang kemudian digunakan untuk kepentingan sendiri, seperti masuk ke sebuah sistem, membuat akun palsu, dan masih banyak lagi. Teknik yang digunakan pelaku kejahatan siber sangatlah beragam seperti *phising, spam,* dan *social engineering* [2]. Tercatat bahwa negara Indonesia berada diperingkat ke-2 dunia kejahatan kasus siber [3]. Kejahatan siber di Indonesia bisa sangat banyak dikarenakan banyak masyarakat yang belum paham tentang bagaimana bentuk kejahatan di dunia siber. Data yang menunjukkan rata-rata kejaharan siber sangat erat kaitannya dengan teknik serangan rekayasa sosial seperti yang dijelaskan sebelumnya.

Dalam berbagai tulisan dinyatakan bahwa manusia adalah elemen yang paling rentan dalam sistem keamanan. [4]. Teknik paling efektif yang digunakan oleh pelaku kejahatan siber yaitu rekayasa sosial. Rekayasa sosial atau biasa dikenal dengan sebutan *social engineering* adalah sebuah teknik yang memanfaatkan kelemahan individu (manusia) untuk memperoleh informasi yang digunakan untuk menerobos sistem keamanan [5]. Mayoritas masyarakat tidak mengetahui cara kerja dari teknik ini, sehingga para pelaku kejahatan siber memperoleh informasi yang diinginkan dengan mudah, bahkan sebagian korban serangan rekayasa sosial tidak sadar bahwa dirinya sedang menjadi target dari pelaku penyerangan rekayasa sosial [6].

Serangan rekayasa sosial pada umumnya menyiratkan interaksi langsung dengan individu lain baik itu bertatap muka langsung atau secara *online*. Pada saat berintaraksi inilah pelaku kejahatan yang menggunakan teknik rekayasa sosial mempengaruhi psikologi korban. Pemahaman yang cukup tentang pemicu-pemicu psikologis dapat mencegah pelaku kejahatan rekayasa sosial [7]. Kasus penyerangan menggunakan teknik rekayasa sosial pertama kali dilakukan oleh Kevin Mitnick yang berasal dari negara Amerika. Mitnick seorang hacker yang hampir tidak menyentuh komputer dalam mengeksploitasi kelemahan targetnya dengan kata lain Mitnick menggunakan teknik rekayasa sosial sepenuhnya [8]. Kevin Mitnick kemudian ditangkap pada tahun 1995 yang kemudian memberikan pernyataan dalam bukunya *The Art of Deception* bahwa *social engineering* adalah bagian yang sederhana dalam pendekatannya. Para pelaku kejahatan dunia siber yang menggunakan teknik rekayasa sosial sangat mahir memanipulasi targetnya dengan berpura-pura menjadi sosok penting dan akrab agar target tidak curiga.

Tidak banyak yang bisa mengetahui proses serangan rekayasa sosial terjadi. Maka dari itu diperlukan perlindungan yang dibentuk dari diri sendiri untuk mengatasi "mata rantai terlemah" pada sistem keamanan yaitu manusia [8]. Perlindungan ini dinamakan *human firewall*. Sama halnya seperti *firewall* yang melindungi jaringan komputer, *human firewall* adalah sebuah bentuk perlindungan yang sengaja dibentuk untuk mencegah berbagai serangan dari *hacker*, terutama serangan yang menggunakan teknik *social engineering*.

Sebagaimana dijelaskan pada paragraf sebelumnya bahwa manusia adalah bagian yang rentan pada sistem keamanan. Pernyataan tersebut sangatlah jelas mengingat bahwa manusia adalah makhluk sosial yang tentu akan berfikir sebelum melakukan tindakan. Tentu, serangan rekayasa sosial yang menyerang individu/manusia sangat merugikan terutama pada perusahaan atau organisasi yang terdiri dari kumpulan individu. Peneliti akan membentuk model *human firewall* dengan menggunakan metode Pohon Keputusan (*decision trees*).

1.2 Rumusan Masalah

Berdasaran latar belakang yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah "Bagaimana membentuk *Human Firewall* menggunakan metode *decision trees* atau pohon keputusan ?".

1.3 Batasan Masalah

Adapun Batasan masa dalam penelitian ini adalah sebagai berikut :

a. Metode yang digunakan dalam penelitian ini adalah *decision trees*.
b. Serangan rekayasa sosial yang dibahas dalam penelitian ini yaitu serangan sosial yang menggunakan pendekatan *physical approaches, social approaches,* dan *technical approaches.*
c. Penelitian mencakup analisis, perancangan model, dan pembuatan model *human firewall.*

1.4 Tujuan Penelitian

Bagian ini memuat penjelasan secara spesifik mengenai:

a. Membangun model *human firewall* menggunakan pohon keputusan.
b. Meningkatkan kehati-hatian dan pengambilan keputusan yang akurat guna mencegah serangan rekayasa sosial.
c. Meningkatkan kesadaran keamanan informasi dan teknologi pada setiap individu.

1.5 Manfaat Penelitian

1.5.1 Bagi Penulis

1. Mengaplikasikan ilmu-ilmu akademis yang didapat selama perkuliahan untuk membangun model *human firewall* menggunakan metode pohon keputusan.
2. Memperluas wawasan khususnya dalam metode *decision trees* untuk membentuk *human firewall.*

1.5.2 Bagi Universitas

1. Memberikan gambaran terhadap penerapan ilmu pengetahuan yang telah diterima selama kuliah.
2. Menjadi sumbangan literatur karya ilmiah dalam disiplin ilmu teknologi khususnya bidang *cyber security*.

Selain itu adapun manfaat pada penelitian ini adalah membantu memberikan edukasi terhadap orang-orang yang memiliki kesadaran keamanan yang rendah untuk membentuk *human firewall* guna mengantisipasi dan menangani serangan rekayasa sosial.

1.6 Metode Penelitian

Dalam melakukan penelitian ada beberapa tahap dan alur penelitian serta metode pengumpulan data untuk mendukung penelitian.

1.6.1 Metode Pengumpulan Data

Peneliti mengumpulkan data dan informasi dengan menggunakan beberapa metode untuk menunjang keberhasilan dari penelitian ini.

1. Metode Observasi

   Pada proses ini peneliti melakukan observasi terkait kejadian yang paling umum terjadi kepada manusia ketika menjadi korban dari serangan rekayasa sosial atau *social engineering attacks*.

2. Studi Literatur

   Pada tahap ini peneliti melakukan pengumpulan data yang diperolah dari buku-buku, jurnal ilmiah, internet, dan juga sumber lain yang berhubungan dengan objek dan metode yang digunakan dalam penelitian ini. Kemudian peneliti membaca dan mempelajari karya-karya ilmiah yang relevan dengan metode *decision trees* beserta mempelajari serangan rekayasa sosial yang paling sering terjadi.

1.6.2 Metode Analisis

Peneliti melakukan analisis terhadap *literatur review* atau studi literatur untuk mendapatkan pehaman mengenai metode yang digunakan yaitu *decision trees* dan pengelompokan serangan rekayasa sosial.

1.6.3 Metode Perancangan

Pada tahap ini peneliti melakukan perancangan sebuah model untuk membentuk *human firewall* dengan menggunakan *metode decision* trees atau pohon keputusan. Pohon keputusan berisi beberapa kejadian yang sangat umum terjadi pada serangan rekayasa sosial (diambil dari penelitian-penelitian sebelumnya).

1.6.4 Metode Implementasi dan Pengujian

Model *human firewall* yang sudah jadi, akan diimplementasikan dengan melakukan tes (pengujian) dalam bentuk kuisioner untuk mengetahui apakah model *human firewall* dapat dipahami dengan mudah dan bisa diterapkan ke individu.

1.7 Sistematika Penulisan

Berisi sistematika penulisan skripsi yang memuat uraian secara garis besar isi skripsi untuk tiap–tiap bab. Penulis harus dapat mendeskripsikan (menggambarkan) apa saja isi masing-masing bab yang akan disusun. Jelaskan secara singkat isi dari bab I, bab II, bab III, bab IV, dan bab V. contoh:

BAB I PENDAHULUAN

pada Bab I berisikan latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Berisi: hasil penelitian sejenis yang sudah pernah dilakukan sebelumnya, teori penunjang, dan referensi berupa buku, jurnal, dan laporan skripsi/tesis.

BAB III METODOLOGI PENELITIAN

Bab III peneliti memaparkan metode yang akan digunakan untuk menunjang proses penelitian hingga selesai. Selain itu, pada Bab

ini terdapat bagian-bagian dari metodologi penelitian yaitu bahan penelitian, alat penelitian, metode penelitian, dan jadwal penelitian.

BAB IV PEMBAHASAN

Pada Bab IV peneliti membahas hasil dari penelitian yang berasal dari pengolahan data. Pada pembahasan ini peneliti juga memberikan model *human firewall* yang sudah dibuat menggunakan metode *decision trees*.

BAB V PENUTUP

Berisi kesimpulan dari hasil akhir penilaian proyek, dan saran yang bermanfaat bagi penulis selanjutnya.