

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pendidikan membantu orang mengembangkan potensi mereka melalui proses pembelajaran (Fitri, 2021). Sebagaimana yang kita ketahui, Pasal 31 Ayat 1 UUD 1945 menyatakan bahwa "setiap warga negara berhak mendapatkan pendidikan." Dengan demikian, pendidikan adalah hak universal. Pendidikan diharapkan dapat menghasilkan generasi penerus yang cerdas dan berkualitas, yang dapat memanfaatkan kemajuan yang telah dicapai. Menurut Pasal 1 Undang-Undang No.20 Tahun 2003 tentang Sistem Pendidikan Nasional, pendidikan didefinisikan sebagai upaya sadar untuk menciptakan suasana belajar di mana peserta didik dapat secara aktif mengembangkan potensi yang dimilikinya selama proses pembelajaran. Diharapkan melalui pendidikan, siswa akan menjadi orang yang cerdas, berakhlak mulia, dan memiliki keterampilan untuk membantu diri mereka sendiri dan masyarakat sekitarnya.

Revolusi Industri 4.0 membawa perubahan besar ke dunia kerja dan banyak aspek kehidupan lainnya, termasuk pendidikan. Kemajuan dalam digitalisasi dan teknologi menjadi kunci utama Revolusi Industri 4.0 karena mempengaruhi bagaimana siswa belajar dan memperoleh keterampilan yang diperlukan untuk menghadapi tantangan di masa depan. Menurut Dito *et al.*, (2021) pendidikan yang merupakan pilar utama dalam kemajuan generasi penerus bangsa harus menyesuaikan diri dengan kemajuan zaman agar tidak tertinggal dari negara maju dalam hal teknologi pendidikan dan kurikulum pembelajaran. Dunia fisik akan

mengalami perubahan besar selama era Industri 4.0 baru, seperti penggunaan fasilitas virtual yang dapat diakses melalui koneksi digital.

Memanfaatkan teknologi dalam pembelajaran adalah cara untuk membantu siswa beradaptasi dengan Revolusi Industri 4.0. Teknologi pendidikan membantu siswa dan guru serta institusi pendidikan secara keseluruhan. Teknologi dapat meningkatkan efisiensi, efektivitas, dan kualitas pembelajaran (Dito & Pujiastuti, 2021). Kemajuan di era digital, pendidikan menghadapi tantangan yang tidak hanya berkaitan dengan akses dan kualitas, tetapi juga keamanan jaringan. Ketergantungan pada teknologi dan internet dalam proses pembelajaran membuat institusi pendidikan rentan terhadap ancaman siber seperti pencurian data, peretasan, dan serangan *malware*. Perubahan yang dimaksud mencakup perkembangan dalam bidang teknologi dasar, kehidupan sosial, dan ekonomi makro, antara lain. Kecerdasan buatan, data *iCloud*, internet orang, *big data*, *internet of things* (IoT), dan digitalisasi adalah beberapa ciri revolusi industri 4.0. Setiap kemajuan ini telah mengubah banyak aspek kehidupan manusia, termasuk salah satu yang paling signifikan, yaitu sektor pendidikan (Afrianto, 2018). *Artificial Intelligence* dan struktur digital fisik mendorong revolusi industri 4.0, yang meningkatkan interaksi manusia-mesin. (Shahroom & Hussin, 2018). Selain itu, industri 4.0 menghadapi kendala saat menjalankan operasinya karena kurangnya budaya digital, pengetahuan, dan bahasa (Hariharasudan & Kot, 2018). Dengan demikian, manusia diharapkan dapat lebih beradaptasi dengan perkembangan revolusi industri sepanjang masa.

Pembangunan pesat jaringan internet umumnya menguntungkan perkembangan teknologi informasi dan komunikasi karena memungkinkan untuk

menghasilkan inovasi yang meningkatkan kemajuan peradaban manusia di era kontemporer. Perkembangan teknologi informasi dan komunikasi di era modern membuat kita selalu bergantung pada manfaat dan kemudahan teknologi tersebut. Teknologi *online* dapat membantu kita melakukan kegiatan sehari-hari kita, dan jika digunakan dengan benar, dapat menjadi cara untuk mendapatkan penghasilan. Namun, kemunculan teknologi internet membuat kita lebih waspada karena risikonya meningkat, terutama ancaman *cyber* (Chirzah & Ramadhan, 2023).

Indonesia adalah salah satu dari banyak negara yang menjadi sasaran serangan siber. Menurut Badan Siber dan Sandi Negara (2021), setiap tahun data yang dicuri mencapai jutaan identitas dan telah mempublikasikan laporan yang diterbitkan pada situs web resmi Direktorat Operasi Keamanan Siber BSSN, Id-SIRTII/CC (*Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center*), menunjukkan bahwa lebih dari 1,6 miliar, atau 1.637.973.022 serangan siber atau anomali trafik, terjadi di seluruh wilayah Indonesia pada tahun 2021.

Menurut Daeng *et al.*, (2023) hal yang perlu diperhatikan adalah bahwa kejahatan *cyber* yang dikenal dengan istilah *hacking* dan *hacker* juga dikenal dengan istilah *cracking* dan *cracker*. Kejahatan yang dilakukan oleh *cracker* atau salah satunya ialah *phising* karena tujuannya untuk menguntungkan diri sendiri dan tentunya merugikan pihak lain jika mereka menjadi korban dari *cybercrime* dalam bentuk *phising*. Salah satu ancaman terhadap keamanan nasional adalah serangan siber. Keamanan nasional sendiri adalah keamanan suatu negara sebagai satu kesatuan dan keamanan orang-orangnya untuk hidup di dalamnya. Perubahan

lingkungan yang dihadapi oleh setiap negara di sistem internasional dapat menjadi sumber ancaman keamanan nasional saat ini.

Keamanan jaringan adalah suatu sistem yang mengidentifikasi pengguna yang tidak memiliki akses ke jaringan untuk mencegah aktivitas yang tidak diinginkan. Ini memungkinkan orang lain untuk melihat, mengubah, atau bahkan menghapus data jaringan. (Purnama, Muhyidin & Singasatia, 2023). Seringkali dianggap bahwa keamanan jaringan dipengaruhi oleh sejumlah faktor, yang bervariasi tergantung pada bahan dasar, tetapi biasanya ada setidaknya beberapa kerahasiaan, integritas, dan ketersediaan adalah konsep dasar keamanan jaringan. Disebabkan oleh tingginya ancaman yang mencurigakan (*suspicious threats*) dan serangan dari internet, sistem keamanan komputer telah menjadi perhatian utama dalam dunia jaringan komputer dalam beberapa tahun terakhir. Keamanan komputer adalah salah satu komponen utama yang dapat memengaruhi tingkat kepercayaan (mencakup kinerja dan ketersediaan) dalam jaringan internet (Rahim, 2016).

Menurut Ramadhani (2023) dalam era di mana teknologi komunikasi dan informasi telah mengubah masyarakat global, masalah keamanan siber semakin kompleks dan mendesak. Sebagai negara dengan populasi internet yang berkembang pesat, Indonesia juga menghadapi ancaman kejahatan siber yang meningkat. Indonesia menggunakan Undang Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai landasan hukum utama untuk menghadapi masalah ini dan mengurangi dampak dan bahaya dari kejahatan siber. Teknologi informasi dan komunikasi tidak hanya memiliki banyak manfaat, tetapi mereka juga dapat

digunakan untuk melakukan tindak kejahatan baru yang dikenal sebagai *cybercrime*, yang membutuhkan perlindungan.

Penyalahgunaan ini menyebabkan peningkatan penggunaan internet di seluruh dunia bersama dengan peningkatan internet, yang dikenal sebagai perang siber atau *cyberwar*. *Cyberwar* atau *cybercrime* adalah setiap aktivitas yang dilakukan seseorang, sekelompok orang, badan hukum, atau entitas yang menggunakan komputer untuk melakukan kejahatan atau menjadikannya sebagai objek kejahatan. Setiap kejahatan tersebut melanggar undang-undang, baik secara substansial maupun formal (Chirzah & Ramadhan, 2023).

Menurut Aidin *et al.* (2016) *honeypot* adalah sebuah sistem atau komputer yang sengaja digunakan sebagai umpan menjadi sasaran digunakan serangan penyerang. *Honeypot* dapat diartikan suatu cara untuk melindungi *Server* dari layanan palsu. Layanan palsu ini telah dikembangkan secara terbuka dan dapat diunduh oleh pengguna tanpa biaya. *Honey Network*, juga dikenal sebagai MHN, adalah sistem manajemen yang dikembangkan oleh Threatstream pada tahun 2014. Sistem ini memiliki banyak sensor *Honeypot* dan memiliki kemampuan untuk menjalankan banyak sensor dalam waktu yang singkat. Selain itu, sistem tersebut memiliki web *interface* yang dapat digunakan untuk menginstal *Honeypot* dan melihat *log* penyerangan. Namun, data yang dihasilkan hanya berupa *log* dan tidak dapat digambarkan dengan cara apa pun, seperti diagram batang atau diagram garis, sehingga pengguna kesulitan membaca pola serangan. Oleh karena itu, sebuah perangkat lunak yang dapat divisualisasikan diperlukan untuk mempermudah visualisasi statistik dan analisis log yang dihasilkan oleh sensor *Honeypot*.

Sistem untuk mendeteksi serangan, yaitu *Intrusion Detection System* (IDS). IDS adalah sebuah sistem yang dirancang untuk mendeteksi serangan atau intrusi pada suatu jaringan atau sistem komputer, dan pendeteksian dilakukan dengan membandingkan pola trafik jaringan dengan pola serangan yang telah diketahui sebelumnya (Sutarti *et al.*, 2018). Salah satu perangkat lunak deteksi intrusi dan menguji stabilitas keamanan sistem yang bersifat *open source* adalah *Pentbox*. Kemampuan yang dimiliki *Pentbox* adalah mampu mengidentifikasi serta mencegah sebuah ancaman serangan terhadap sistem atau pada *Honeypot* dengan menggunakan aturan yang terintegrasi. Alur kerja dari *Pentbox* adalah sebuah *tool open source* yang menerapkan sistem simulasi dan memantau keamanan jaringan serta aktivitas serangan. Alat ini berfungsi pada *Honeypot* yaitu sistem yang sengaja dibuat untuk menarik perhatian pihak yang tidak bertanggung jawab. Jika pada *Server* terdapat serangan, *Honeypot* juga membantu untuk menyimpan aktivitas tersebut.

SMK YPM 1 Taman yang berada di Kabupaten Sidoarjo merupakan institusi yang bergerak di bidang Pendidikan. Salah satu fasilitas pendukung terdapat jurusan Teknik Komputer dan Jaringan serta menyediakan laboratorium dan internet. Berdasarkan observasi dan wawancara yang dilakukan pada tanggal 8 Oktober 2024 dengan Bapak Muchammad Ichiya' Ulumuddin, S.Kom selaku Kepala Laboratorium yang sering menangani masalah jaringan komputer sekolah, memberitahukan bahwa di SMK YPM 1 Taman kurangnya keamanan jaringan yang diterapkan. Beliau memaparkan bahwa keamanan jaringan yang ada hanya berasal dari *Server* pusat atau bawaan dari *Router*, sehingga administrator tidak dapat mendeteksi adanya serangan ketika jaringan bermasalah. Beliau juga menceritakan

bahwasannya pada *Server* sekolah pernah mengalami serangan secara ilegal oleh pihak yang tidak bertanggung jawab dan tidak dapat mendeteksi adanya serangan, tetapi beliau menyampaikan hanya melakukan *troubleshooting* pada jaringan komputer saja.

Berdasarkan hasil observasi, SMK YPM 1 Taman yang memiliki *Server* dan puluhan PC yang terkoneksi dengan jaringan internet. Maka dari itu, perlu untuk meningkatkan keamanan jaringan seperti pendeteksian lalu lintas data dan paket akses yang masuk. Dengan jumlah perangkat yang terkoneksi ke internet semakin banyak, resiko anomali atau aktivitas yang mencurigakan bisa saja terjadi lagi. Oleh karena itu, sekolah bisa saja berpotensi mengalami gangguan pada jaringan *wireless* yang digunakan.

Hasil penelitian oleh Firdaus (2020), yang bertujuan untuk mengimplementasikan *Honeypot* untuk *Intrusion Detection* menggunakan *Pentbox*. Hasil penelitian yang didapatkan adalah log *Honeypot* mendeteksi informasi perangkat yang digunakan serta merespon dengan cepat ketika ada penyerang pada *port* yang akan diserang.

Penelitian yang dilakukan oleh Asadullah (2019), meneliti dan menerapkan sistem keamanan *Server* dengan *Honeypot* dan *Intrusion Detection System* (IDS). Hasil penelitian yang didapat adalah kombinasi *Honeypot* dan IDS secara otomatis akan menampilkan *message box* dan dapat mendeteksi *IP Address* dan memberikan sistem keamanan berlapis.

Penelitian yang relevan selanjutnya dilakukan oleh Faldi *et al.*, (2023), yang melakukan penelitian dengan tujuan untuk mengimplementasikan *Honeypot* dan *Pentbox* sebagai *Intrusion Detection System*. Penelitian ini menggunakan pengujian

keamanan jaringan dengan beberapa skenario penyerangan yaitu *Web Server* dan *DDoS Attack*. Persamaan dari penelitian ini yakni menggunakan *Honeypot* sebagai *Server Jaringan* dan *Pentbox* sebagai menguji stabilitas keamanan *Server* dan *Intrusion Detection System*.

Berdasarkan hasil observasi, wawancara, dan penelitian relevan tersebut maka peneliti menerapkan keamanan jaringan menggunakan *Intrusion Detection System* berbasis *Pentbox* dalam mendeteksi dan mencegah penyerangan layanan *Server* pada jaringan wireless di SMK YPM 1 Taman. Berdasarkan penelitian yang dilakukan Faldi *et al.*, (2023) yang menerapkan *Honeypot* dan *Pentbox*, peneliti mengutip beberapa serangan yang akan diujicobakan pada penelitian ini yakni *MySQL Server* dan *FTP Server*. *Pentbox* akan dibangun dalam sistem operasi Linux. Dan peneliti pun tertarik untuk melakukan penelitian dengan judul **“Implementasi *Honeypot* dengan Model *Honey Network* dan *Intrusion Detection System* Menggunakan *Pentbox* pada Jaringan *Wireless*”**.

1.2 Rumusan Masalah

Berdasarkan terhadap latar belakang yang sudah diuraikan diatas, peneliti menentukan rumusan masalah seperti berikut :

1. Bagaimana implementasi *Intrusion Detection System* berbasis *Pentbox* sebagai keamanan jaringan *wireless* terhadap penyerangan?
2. Bagaimana hasil pengujian di SMK YPM 1 Taman terkait *Intrusion Detection System* berbasis *Pentbox* sebagai keamanan jaringan *wireless* terhadap penyerangan?

1.3 Tujuan Penelitian Pengembang

1. Untuk mengimplementasikan *Instrusion Detection System* berbasis *Pentbox* sebagai keamanan jaringan wireless terhadap penyerangan.
2. Untuk mengetahui hasil pengujian *Instrusion Detection System* berbasis *Pentbox* sebagai keamanan jaringan *wireless* terhadap penyerangan.

1.4 Spesifikasi Produk yang Diharapkan

Spesifikasi produk yang peneliti harapkan pada penelitian ini adalah sebagai berikut:

1. *Pentbox* adalah *Software* atau *tool* yang bersifat sumber terbuka, dapat digunakan untuk mendeteksi dan mencegah ancaman pada jaringan komputer.
2. Linux Debian *Server* adalah Sistem Operasi yang digunakan untuk menginstall *Honeypot*.
3. Komputer *Client* adalah sebuah perangkat keras yang akan digunakan sebagai lokasi untuk menerapkan *Pentbox*.
4. *Tools Honeypot* adalah sebuah alat yang akan peneliti gunakan untuk menguji.
5. *Software Virtual Box* adalah alat untuk membuat virtualisasi didalam sebuah komputer, disini peneliti akan gunakan untuk diisikan operasi sistem debian sebagai tempat penginstallan *Honeypot* dan *Pentbox*.

1.5 Batasan Penelitian Pengembangan

Terdapat beberapa batasan masalah pada skripsi ini, yaitu :

1. Implementasi dilakukan pada jaringan wireless berbasis *Server – client*.
2. Penelitian ini hanya dilakukan di Sekolah SMK YPM 1 Taman.
3. Penerapan menggunakan sistem operasi Linux dan perangkat lunak *Honeypot* dan *Pentbox*.

4. Layanan yang digunakan untuk penyerangan yaitu *Web Server* dan *FTP Server*.
5. Pengujian serangan dilakukan dalam beberapa tahapan yaitu menguji pengujian keamanan *Server* menggunakan *Honeypot*, *IDS* dan *Pentbox*.

1.6 Pentingnya Penelitian Pengembangan

Adapun manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Manfaat Teoritis

Sistem keamanan yang diteliti efektif sehingga menjadi pendukung untuk penelitian selanjutnya.

2. Manfaat Praktis

- a. Bagi peneliti, implementasi *Honeypot* dengan model *honey network* dan *IDS* menggunakan *Pentbox* pada jaringan *wireless* dapat meningkatkan pengetahuan peneliti dalam menangani masalah keamanan yang sering terjadi dalam infrastruktur jaringan.
- b. Bagi pembaca, implementasi keamanan jaringan dapat pengembangan ilmu pengetahuan dan meningkatkan kesadaran masyarakat akan pentingnya keamanan siber, terutama dalam konteks jaringan nirkabel yang semakin luas penggunaannya.

1.7 Definisi Istilah

1. Sistem deteksi intrusi (*IDS*) dapat mendeteksi aktivitas mencurigakan dalam sistem atau jaringan.
2. *Honeypot* adalah sebuah sistem atau *Server* yang digunakan sebagai umpan untuk tujuan serangan *hacker* (*attacker*).

3. Keamanan jaringan adalah sistem pertahanan terhadap jaringan dan aplikasi-aplikasinya terhadap serangan atau aktivitas yang berpotensi membahayakan keabsahan dan integritas data.
4. *Pentbox* adalah sistem *open source* yang menyediakan alat – alat keamanan jaringan komputer untuk melindungi dari serangan pada jaringan.