BAB I

PENDAHULUAN

1.1 Latar Belakang

Sejalan dengan berkembangnya zaman, teknologi informasi dan komunikasi telah berkembang dengan sangat pesat sehingga memiliki peran penting dalam kehidupan masyarakat dan menjadi suatu layanan yang sangat dibutuhkan di berbagai sektor, baik di instansi pemerintahan, perkantoran maupun perusahaan. Salah satu teknologi yang mengalami perkembangan signifikan adalah jaringan komputer yang berkembang dalam bidang transmisi data, jaringan komputer memiliki 2 jenis media transmisi data, yaitu berupa kabel dan nirkabel yang memungkinkan penggunaan secara bersama data dan perangkat untuk saling terhubung satu dengan yang lain sehingga mempermudah kelompok kerja dalam berkomunikasi dan berbagi sumber daya dengan lebih efisien (Simanjuntak, Sugianto, Asyarie, & Lan, 2019).

PT. Pupuk Sriwidjaja, sebagai perusahaan yang terus berkembang dan beradaptasi dengan perubahan zaman, menyadari betapa pentingnya jaringan komputer dalam mendukung kelancaran operasionalnya. Dalam upaya meningkatkan efisiensi kerja dan produktivitas, PT. Pupuk Sriwidjaja berkomitmen untuk menyediakan fasilitas jaringan komputer yang handal bagi seluruh karyawan dan pekerjanya. Dengan adanya jaringan komputer, berbagai departemen, bagian, dan unit kerja dapat berkomunikasi serta bertukar informasi dengan cepat dan akurat, serta memudahkan dalam hal pengelolaan data dan berbagi file atau

dokumen. Mengingat peranannya yang sangat penting membuat PT. Pupuk Sriwidjaja membentuk Departemen TI yang terdiri dari 3 bagian, yaitu Bagian Infrastruktur TI untuk melakukan perencanaan dan pengembangan infrastruktur TI, Bagian Tata kelola TI untuk membantu Departemen TI, dan Bagian Layanan TI untuk melakukan penyediaan dukungan IT *Helpdesk*.

Bagian Layanan TI PT. Pupuk Sriwidjaja memiliki 3 ruangan utama, yaitu ruang AVP, ruang teknisi, dan ruang kerja praktik. Di ruang kerja praktik, terdapat jaringan *Wireless Local Area Network* (WLAN) yang keamanannya terpisah dari jaringan pada gedung utama atau jaringan pusat PT. Pupuk Sriwidjaja. Kondisi yang terpisah ini membutuhkan perlindungan yang juga berbeda, sehingga berpengaruh terhadap keamanannya. Saat peneliti sedang melakukan penelitian, ruang kerja praktik dilengkapi dengan dua perangkat jaringan yaitu sebuah *wireless router Tenda* yang diatur dalam mode *access point* (AP) dan sebuah *router MikroTik* RB941. *Wireless router Tenda* berfungsi untuk menyediakan koneksi internet melalui jaringan *Wi-Fi* yang digunakan oleh beberapa perangkat pengguna termasuk *smartphone* dan *laptop* yang digunakan untuk mengakses internet. *Wireless router Tenda* dan *Router MikroTik* terhubung pada segmen jaringan yang sama, namun memiliki perbedaan dalam hal keamanan, yang mana *wireless router Tenda* menerapkan protokol keamanan standar jaringan WLAN yaitu protokol *Wi-Fi Protected Access* 2-*Pre Shared Key* (WPA2-PSK) untuk melindungi keamanan pengguna *wireless*-nya, sementara pada *router MikroTik* belum menerapkan atau mengaktifkan keamanan apapun selain hanya digunakan untuk mengelola dan mengontrol akses pengguna jaringan WLAN yang terhubung melalui *wireless*

router Tenda. Kondisi ini menimbulkan potensi risiko keamanan, karena *router MikroTik* yang tidak terlindungi dapat menjadi celah keamanan atau titik lemah dalam jaringan WLAN.

Berdasarkan kondisi tersebut, peneliti melakukan pengujian terhadap tingkat keamanan jaringan WLAN di ruang kerja praktik menggunakan teknik *vulnerability scanning*. Pengujian ini berfokus untuk mendeteksi potensi kerentanan yang ditemukan, dengan hasil pengujian awal *vulnerability scanning* sebagai berikut:

Gambar 1.1 Pengujian awal *vulnerability scanning*

Seperti terlihat pada gambar 1.1, dari indikator yang diwarnai terdapat keterangan setiap informasi, warna jingga menunjukan kategori *Medium* dengan dampak yang tidak terlalu tinggi juga tidak rendah, warna kuning menunjukan kategori *Low* dengan dampak yang minim jika dieksploitasi, dan warna biru menunjukan *Info* yang tidak menunjukan adanya kerentanan. Selain itu, terdapat juga indikator berwarna lain yaitu warna merah menunjukan *Critical* yang jika dieksploitasi dapat menyebabkan kerusakan serius pada sistem dan warna jingga gelap menunjukan *High* yang jika dieksploitasi juga menyebabkan dampak yang cukup serius.

Tabel 1.1 Hasil pengujian awal *vulnerability scanning*

No	Kategori	*Title*	*Family*	*Port/Service*
1	*Medium*	*Unencrypted Telnet Server*	*Misconf*	*23/Telnet*
2	*Low*	*SSH Multiple Issue*	*Misconf*	*22/SSH*
3	*Info*	*MikroTik Neighbor Discovery Protocol Detection*	*Service Detection*	*5678/MNDP*
4	*Info*	*MikroTik RouterOS Detection*	*Service Detection*	*80/www*
5	*Info*	*SSH Multiple Issue*	*Service Detection*	*22/SSH*
6	*Info*	*Nessus Syn Scanner*	*Port Scanner*	*21/22/23/53/80 /8080*
7	*Info*	*Service Detection*	*Service Detection*	*21/22/23/80*
7	*Info*	*DNS Server Detection*	*DNS*	*53/TCP/UDP/ DNS*
8	*Info*	*FTP Server Detection*	*Service Detection*	*21/FTP*
9	*Info*	*SSH Protocol Version Supported*	*General*	*22/SSH*
10	*Info*	*Telnet Server Detection*	*Service Detection*	*23/Telnet*

Berdasarkan hasil yang tercantum pada tabel 1.1, terdapat 7 *port* yang terdeteksi terbuka, seperti pada *port* 21 *FTP*, *port* 22 *SSH*, *port* 23 *Telnet*, *port* 53 *DNS* pada protokol *TCP* dan *UDP*, *port* 80 *HTTP*, dan *port* 8080 alternatif *HTTP*. Selain itu, diketahui juga bahwa pada *port* 5678 yaitu *service MikroTik Neighbor Discovery Protocol* (*MNDP*) yang terbuka. Dari hasil pengujian awal *vulnerability scanning*, teridentifikasi 3 kategori tingkat kerentanan yang berbeda, yaitu kerentanan dengan kategori *medium*, kerentanan dengan kategori *low*, dan kategori *info*. Temuan ini menunjukan bahwa keamanan jaringan WLAN di ruang kerja praktik masih memiliki kelemahan yang berpotensi untuk dieksploitasi.

Peneliti berupaya mencari solusi untuk mengatasi permasalahan yang ditemukan, yaitu kerentanan yang diperoleh dari pengujian awal *vulnerability scanning.* Solusi yang dilakukan peneliti adalah dengan menerapkan *hardening* yang akan dikonfigurasikan pada *router MikroTik* untuk mengoptimalkan sistem keamanan jaringan WLAN, yaitu dengan menutup dan menyamarkan celah-celah kerentanan yang ditemukan serta memperkuat ketahanan jaringan agar lebih resisten terhadap gangguan dan serangan. Tindakan *hardening* yang diterapkan peneliti mencakup pembatasan akses *services* pada *port* 21 *FTP*, *port* 22 *SSH*, dan 80 *HTTP* yang diatur untuk hanya bisa diakses oleh IP *Address* dalam *network* 192.168.10.0/24, menerapkan *firewall raw* dan *firewall filter* pada *port* 53 *DNS*, menonaktifkan akses *services* pada *port* 23 *Telnet* dan *port* 8080 alternatif *HTTP*, menonaktifkan *service MikroTik Neighbor Discovery Protocol* pada *port* 5678, dan menerapkan teknik *port knocking* sebagai lapisan keamanan tambahan pada *port* 22 *SSH* yang sedang dijalankan.

Berdasarkan uraian di atas, terkait adanya permasalahan yaitu kerentanan yang ditemukan pada jaringan WLAN di ruang kerja praktik pada Bagian Layanan TI PT. Pupuk Sriwidjaja, untuk itu peneliti akan menerapkan *hardening* sebagai upaya dan tindak lanjut untuk mengoptimalkan keamanan jaringan WLAN. Oleh karena itu, judul yang diambil peneliti dalam penelitian ini adalah "**Penerapan Hardening untuk Optimalisasi Keamanan WLAN Bagian Layanan TI pada PT. PUSRI**"

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka dapat dirumuskan suatu permasalahan, yaitu "Bagaimana cara menerapkan *hardening* dengan tujuan agar keamanan jaringan WLAN di Bagian Layanan TI Pupuk Sriwidjaja menjadi lebih optimal" yang didasari dengan permasalahan yang terdapat pada lokasi penelitian, khususnya di ruang kerja praktik pada Bagian Layanan TI Pupuk Sriwidjaja.

1.3 Batasan Masalah

Agar penelitian yang dilakukan lebih terfokus maka perlu adanya suatu batasan. Berikut adalah batasan masalah yang akan diberlakukan dalam dalam penelitian ini.

1. *Vulnerability scanning* untuk menguji tingkat keamanan jaringan WLAN dilakukan sebelum dan sesudah penerapan *hardening*.
2. *Hardening* mencakup penerapan *firewall filter* pada *services port* 21, 22, dan 80 yang diatur untuk hanya dapat diakses oleh *network* yang ditentukan, menerapkan *firewall raw* dan *firewall filter* terhadap *port* 53 *DNS* pada protokol *TCP* dan *UDP*, menonaktifkan *services* pada *port* 23 dan *port* 8080 dengan menerapakan *firewall filter* dengan *action tarpit*, menonaktifkan *service mikrotik neighbor discovery protocol port* 5678, dan menerapkan *port knocking* terhadap *port* 22.
3. Penggunaan *tools Nessus* dan *winbox* sebagai dukungan dalam melakukan *vulnerability scanning* dan menerapkan *hardening* pada jaringan WLAN.
4. Penelitian hanya berfokus di ruang kerja praktik pada Bagian Layanan TI Pupuk Sriwidjaja.

1.4 Tujuan Penelitian

Adapun tujuan dari penerapan *hardening* ini adalah untuk mengurangi dan meminimalisir risiko kerentanan yang ditemukan, serta untuk mengoptimalkan sistem keamanan jaringan WLAN dari berbagai ancaman dan serangan yang dapat merugikan pengguna jaringan WLAN pada Bagian Layanan TI Pupuk Sriwidjaja.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat bagi berbagai pihak, baik yang terlibat secara langsung maupun tidak langsung. Berikut adalah beberapa manfaat yang dapat diperoleh.

1. Mengetahui bagaimana langkah-langkah yang efektif dalam menerapkan *hardening* untuk mengoptimalkan dan memperkuat ketahanan jaringan WLAN di ruang kerja praktik terhadap potensi serangan dan gangguan.
2. Membuat pengguna jaringan WLAN merasa aman karena adanya pembatasan pengguna dalam mengakses jaringan .
3. Hasil penelitian ini dapat memberikan wawasan yang mendalam terkait penerapan *hardening* dalam meningkatkan keamanan jaringan WLAN serta dapat menjadi acuan bagi penelitian-penelitian selanjutnya mengenai tindakan *hardening* dalam melindungi jaringan WLAN.

1.6 Penelitian Terdahulu

Penelitian terdahulu merupakan analisis terstruktur yang menguraikan informasi yang sebelumnya telah dilakukan oleh peneliti lain yang memiliki

relevansi dengan masalah penelitian yang sedang diteliti. Berikut adalah penelitian terdahulu yang menjadi pembanding dalam penelitian ini.

(Hanipah & Dhika, 2020) dalam penelitian yang berjudul "Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark", Tujuan dari penelitian ini mendeteksi serangan di dalam jaringan, metode yang digunakan adalah *vulnerability scanning* menggunakan tools wireshark. Hasil penelitian menunjukan bahwa data yang berhasil dianalisis dari pemfilteran paket data memungkinkan administrator jaringan untuk melakukan analisis terhadap paket-paket jaringan yang masuk.

(Putri, Agita, & Soim, 2023) dalam penelitian yang berjudul "Implementasi *Port Knocking*, *Port Blocking* Pada Keamanan Jaringan Komputer Berbasis Mikrotik", tujuan dari penelitian ini adalah meningkatkan keamanan akses pengguna komputer dari risiko pencurian data dan informasi serta menjaganya agar tetap aman. Metode yang digunakan ialah *port knocking* dan *port blocking*, dengan hasil penelitian menunjukan bahwa pengguna perlu melakukan autentikasi ke *port* khusus untuk meningkatkan keamanan *server*.

Penelitian yang dilakukan oleh (Firmansyah, Purnama, & Astuti, 2021) yang berjudul "Optimalisasi Keamanan Wireless Menggunakan Filtering MAC *Address"*, tujuan dari penelitian untuk ialah untuk meningkatkan keamanan baik untuk pengguna maupun jaringan dengan menghalangi akses ilegal dari pengguna yang tidak sah yang melakukan percobaan akses ke dalam jaringan. Metode yang digunakan ialah SPDLC atau *Security Policy Development Life Cycle*. Dengan hasil

penelitian, yaitu untuk klien yang telah didaftarkan MAC *Address*nya dapat terhubung ke dalam jaringan internet.

Merujuk pada penelitian yang dilakukan (Haris et al., 2022) dengan judul "Analisis Pengamanan Jaringan Menggunakan *Router* Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi", Tujuan dari penelitian ini adalah untuk mengevaluasi pengamanan jaringan dari serangan DDoS menggunakan *router* mikrotik dengan memanfaatkan fitur-fitur yang ada sehingga keefektifannya dapat dinilai. Metode yang dipakai, yaitu PPDIO atau *Prepare, Plan, Design, Implement, Operate,* dan *Optimize*. Hasil penelitian menunjukan penurunan konsumsi CPU sebesar 20% dan *ping response time* berhasil pulih ke kondisi normal, sementara sistem deteksi dan blokir serangan bekerja secara otomatis.

(Adrian & Cahyana, 2022) dalam penelitian yang berjudul "Perancangan Arsitektur Jaringan Kampus Menggunakan *Metode Network Development Life Cycle"*, penelitian ini bertujuan untuk merancang arsitektur jaringan komputer menggunakan metode *Network Development Life Cycle* yang mencakup analisis, perancangan, dan simulasi. Hasil simulasi menunjukan pernyesuaian kondisi jaringan sesuai dengan kebutuhan karena desain infrastruktur dan keamanan jaringan telah diperbarui mengikuti perkembangan teknologi saat itu, diantaranya dengan menubah *username* dan *password login default* serta menonaktifkan *neighbor discovery* pada interface yang mengarah ke publik.

Penelitian yang dilakukan (Setiayoko, Swanjaya, & Farida, 2023) dengan judul "Analisis Implementasi *Port Knocking* pada Keamanan Jaringan di SMK PGRI 1 Nganjuk", penelitian ini bertujuan untuk meningkatkan keamanan jaringan

internet dengan menutup akses *port* dan menambahkan fungsi anti DDoS. Metode yang digunakan, yaitu *port knocking* dan anti DDoS. Setelah dilakukan pengujian sistem, hasil penelitian menunjukan bahwa konfigurasi *port knocking* berfungsi dengan baik, yaitu ketika *router* dalam kondisi keamanan yang sudah diterapkan *port scan* dan *sniffing* tidak dapat dilakukan. Selain itu, menerapkan teknik mitigasi DDoS dapat mengurangi risiko penyalahgunaan akses *router* oleh pihak yang tidak bertanggung jawab.