BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang semakin berkembang pesat, konektivitas nirkabel, khususnya jaringan *Wi-Fi*, telah menjadi infrastruktur penting dalam berbagai organisasi, termasuk Direktorat Inovasi dan Inkubator Bisnis (DIIB). *Wi-Fi* (*Wireless Fidelity*) adalah sebuah teknologi yang memungkinkan perangkat elektronik, seperti komputer, *smartphone*, atau tablet, untuk terhubung ke jaringan internet atau jaringan lokal (*LAN*) tanpa menggunakan kabel fisik. *Wi-Fi* menggunakan teknologi standar *IEEE 802.11* untuk mentransmisikan data melalui gelombang radio, yang memungkinkan akses internet dan komunikasi nirkabel secara praktis dan efisien (Suroto, 2018). *Wi-Fi* memberikan kemudahan akses internet yang diperlukan oleh staf, mahasiswa, pengunjung, dan berbagai perangkat yang terhubung ke jaringan, yang semuanya berperan penting dalam mendukung aktivitas sehari-hari dan inovasi di Direktorat Inovasi dan Inkubator Bisnis (DIIB).

Namun, keberadaan jaringan *Wi-Fi* tidak luput dari serangan-serangan siber yang dilakukan oleh pihak yang tidak bertanggung jawab yang bisa berakibatkan merugikan orang lain (Adiguna & Widagdo, 2022). Berdasarkan data Badan Siber dan Sandi Negara (BSSN) pada tahun 2022, Indonesia mencatat terdapat sekitar 370,02 juta insiden serangan siber. Angka ini menunjukkan peningkatan sebesar 38,72% dari tahun sebelumnya, di mana tercatat sekitar 266,74 juta serangan siber di Indonesia (Pratiwi, 2022). Maka dari itu, Keamanan jaringan *Wi-Fi* menjadi hal

yang krusial mengingat banyaknya data sensitif dan informasi rahasia yang dapat diakses melalui jaringan ini. Ancaman keamanan seperti peretasan (*hacking*), pencurian data, dan serangan berbagai jenis semakin mengintensifkan kebutuhan untuk melindungi *Wi-Fi* (Haeruddin & Kurniadi, 2021).

Direktorat Inovasi dan Inkubator Bisnis (DIIB) merupakan sebuah direktorat pada Universitas Bina Darma yang fokus pada pengembangan inovasi dan memberikan dukungan bagi pertumbuhan bisnis dari inovasi mahasiswa dan dosen. DIIB juga menggunakan jaringan *Wi-Fi* sebagai infrastruktur untuk membantu dalam memenuhi kebutuhan informasi seperti mengakses internet, membuka sosial media, melakukan transaksi *online* dan sejenisnya**.** Jaringan *Wi-Fi* yang disediakan Direktorat Inovasi dan Inkubator Bisnis telah menerapkan sistem keamanan WPA2-PSK pada *access point* yang digunakan untuk dapat terhubung ke jaringan tersebut. Namun, penggunaan keamanan WPA2-PSK saja pada *Wi-Fi* tanpa adanya konfigurasi keamanan tambahan masih memiliki banyak celah yang dapat dieksploitasi dengan meningkatnya tingkat kompleksitas serangan siber dan beragamnya teknik yang digunakan oleh para penyerang, hal ini sangat berbahaya bagi pengguna jaringan *Wi-Fi* di DIIB dikarenakan tidak menutup kemungkinan adanya serangan pada jaringan tersebut.

Berdasarkan permasalahan diatas, mengidentifikasi kelemahan keamanan dalam jaringan adalah langkah penting untuk menghadapi ancaman yang ada. Dalam hal ini, pengujian penetrasi *(penetration testing)* menjadi metode yang efektif untuk menguji dan mengekspos kelemahan keamanan dalam suatu sistem atau jaringan (Wahyudi, Luthfi, & Efendi, 2019). *Penetration testing* pada *Wi-Fi*

melibatkan upaya yang disengaja untuk menguji keamanan jaringan *wireless* dengan menggunakan teknik dan metode yang serupa dengan serangan yang dapat dilakukan oleh penyerang seperti serangan *Denial of Service, Password Cracking, Spoofing*, dan *Man in the Middle* (*MITM*). (Eval Agustin Martin, 2021).

Dalam melakukan *Penetration testing*, penggunaan berbagai *tools* menjadi kunci dalam mensimulasikan serangan untuk menguji tingkat keamanan suatu sistem atau jaringan. Untuk menjalankan *penetration testing* secara efektif terhadap jaringan *Wi-Fi* diperlukan *tools* yang memiliki fungsionalitas beragam, seperti pemindaian jaringan, eksploitasi, dan pemantauan (Kongara, 2023). Kali Linux adalah distribusi Linux yang khusus dikembangkan untuk tujuan *penetration testing* dan keamanan komputer (Rusdi & Prasti, 2019). Kali linux menyediakan banyak *tools* dan aplikasi yang telah diintegrasikan secara *default* untuk mendukung aktivitas *penetration testing*. Di dalamnya, terdapat beragam *tools* penting yang siap digunakan untuk melakukan *penetration testing* pada jaringan *Wi-Fi* seperti *aircrack-ng*, *wireshark* dan *tools* lainnya (Kyei & Asante, 2020).

Penelitian ini bertujuan mengimplementasi *tools penetration testing* untuk menguji sejauh mana tingkat keamanan jaringan *Wi-Fi* yang diterapkan pada Direktorat Inovasi dan Inkubator Bisnis, terutama dalam menghadapi ancaman serangan siber yang berpotensi mengganggu dan merugikan para pengguna. Dalam penelitian ini akan dilakukan praktik *penetration testing* dengan mensimulasikan beberapa jenis serangan, termasuk *Denial of Service*, peretasan enkripsi (*Cracking The Encryption*), *MAC Spoofing*, serta *Man-in-the-Middle* menggunakan *tools* yang tersedia dalam sistem operasi kali linux. Dengan demikian, penelitian ini secara

khusus bertujuan untuk mengetahui potensi celah keamanan yang dapat dieksploitasi oleh berbagai serangan jaringan *wireless* yang berpotensi mengancam pada *Wi-Fi* yang digunakan oleh Direktorat Inovasi dan Inkubator Bisnis.

Penelitian sebelumnya telah banyak melakukan *penetration testing* untuk menguji keamanan jaringan *Wi-Fi.* Sebagai contoh, penelitian oleh (Lu & Yu, 2021) menunjukan hasil percobaan bahwa metode pengujian penetrasi jaringan *Wi-Fi* dengan Kali Linux berpengaruh baik dalam meningkatkan evaluasi keamanan jaringan *Wi-Fi*. Penelitian yang dilakukan oleh (Saraun, Lumenta, & Sengkey, 2022) juga mengidentifikasi serangan yang umumnya dalam jaringan *Wi-Fi* dengan menggunakan metode *penetration testing* dan memberikan data sebagai bahan untuk memperkuat keamanan jaringan.

Berdasarkan uraian diatas peneliti akan mengangkat judul **"Implementasi Tools Penetration Testing Untuk Menguji Tingkat Keamanan Wi-Fi pada Direktorat Inovasi dan Inkubator Bisnis."**

1.2 Perumusan Masalah

Dari uraian latar belakang yang sudah dijelaskan diatas dapat diambil rumusan masalah yaitu:

1. Bagaimana mengimplementasikan *tools penetration testing* untuk menguji tingkat keamanan *Wi-Fi* pada Direktorat Inovasi dan Inkubator Bisnis?
2. Serangan apa saja yang dapat dieksploitasi pada *Wi-Fi* yang digunakan oleh Direktorat Inovasi dan Inkubator Bisnis?

1.3 Batasan masalah

Agar lebih fokus terhadap masalah yang di teliti, maka diberikan batasan sebagai berikut:

1. Pengujian ini akan difokuskan pada jaringan *Wi-Fi* yang digunakan oleh Direktorat Inovasi dan Inkubator Bisnis..
2. Penelitian tidak akan membahas aspek keamanan jaringan yang lain, seperti jaringan kabel atau infrastruktur jaringan lainnya.
3. Pengujian serangan yang akan penulis lakukan hanya *Denial of Service* (DoS), *Cracking The Encryption*, *MAC Spoofing*, dan *Man in the Middle* (*MITM*).

1.4 Tujuan penelitian

Adapun tujuan dari penelitian yang dilakukan ini adalah sebagai berikut:

1. Melakukan Implementasi *tools penetration testing* untuk menguji tingkat keamanan *Wi-Fi* Direktorat Inovasi dan Inkubator Bisnis.
2. Mengetahui serangan - serangan yang dapat dieksploitasi pada *Wi-Fi* yang digunakan oleh Direktorat Inovasi dan Inkubator Bisnis.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah:

1. Manfaat terhadap peneliti

   Peneliti akan mendapatkan pengalaman dan pengetahuan yang lebih dalam mengenai keamanan jaringan dan pengujian penetrasi. Peneliti akan mengembangkan keterampilan teknis dalam penggunaan *tool penetration*

testing dan analisis keamanan. Hal ini dapat meningkatkan keahlian peneliti di bidang keamanan informasi dan membuka peluang karir di bidang keamanan teknologi.

2. Manfaat terhadap Direktorat Inovasi dan Inkubator Bisnis

   Diharapkan dengan adanya hasil dari penelitian ini bisa menjadi data yang dapat digunakan oleh pihak Direktorat Inovasi dan Inkubator Bisnis guna untuk mengamankan jaringan *Wi-Fi* dari orang-orang yang menyalahgunakan layanan yang telah disediakan dan sebagai pengetahuan bagi pengguna akan bahaya dari pemakaian jaringan *Wi-Fi*.

3. Manfaat terhadap pembaca

   Diharapkan dengan adanya penelitian ini dapat menjadi sebuah informasi serta referensi dalam mengamankan jaringan *wireless* serta penggunaan *tools penetration testing*.

1.6 Penelitian Terdahulu

Penelitian yang dilakukan (Lu & Yu, 2021) berjudul "*Research on WiFi Penetration Testing with Kali Linux*" dalam penelitian ini, penulis bertujuan untuk mencari kerentanan jaringan nirkabel, artikel ini mengusulkan metode pengujian penetrasi *Wi-Fi* berbasis Kali Linux yang dibagi menjadi empat tahap: persiapan, pengumpulan informasi, serangan simulasi, dan pelaporan. Dengan menggunakan metode *monitoring*, *scanning*, *capture*, analisis data, *password cracking*, f*ake wireless access point spoofing*, dan metode lainnya, pengujian penetrasi jaringan *Wi-Fi* dengan *Kali Linux* diproses di lingkungan simulasi. Hasil percobaan

menunjukkan bahwa metode pengujian penetrasi jaringan *Wi-Fi* dengan Kali Linux berpengaruh baik dalam meningkatkan evaluasi keamanan jaringan *Wi-Fi.*

Dalam penelitian yang dilakukan (Saputra, Kom, Saputra, & Zen, 2023) berjudul "Analisis Keamanan Jaringan *Wireless* menggunakan Metode *Penetration Testing Execution Standard* (PTES)" dalam penelitian ini, dilakukan analisa keamanan jaringan dengan menggunakan metode *Penetration Test Execution Standard* (PTES) yang merupakan suatu kerangka kerja atau arahan. penetrasi. Berdasarkan hasil 5 kali pengujian menggunakan mesin *virtual* OS Kali Linux dengan serangan *bypassing mac authentication, arp spoofing* masing-masing berstatus berhasil sedangkan *cracking the encryption* berstatus 3 kali gagal dan 2 kali berhasil. Berdasarkan hasil pengujian dapat disimpulkan bahwa sistem keamanan jaringan nirkabel cukup aman, namun demikian diperlukan beberapa perbaikan pada konfigurasi sistem dan topologi jaringan untuk memperkuat sistem keamanan dan mengurangi ancaman kejahatan.

Dalam penelitian yang dilakukan (Sitompul et al., 2023) berjudul "Analisis Penerapan Metode Penetration Testing Pada Keamanan Jaringan Wlan (Studi Kasus: Universitas Maritim Raja Ali Haji)" dalam penelitian ini, penulis melakukan analisis terhadap kelemahan keamanan yang umumnya terkait dengan jaringan *Wi-Fi*. Penelitian ini mengimplementasikan serangan terhadap jaringan *Wi-Fi*, seperti serangan *Bypassing MAC Authentication, Attacking the Infrastructure dan Man in the middle attack*. Hasil penelitian ini memberikan wawasan yang berguna dalam memahami kerentanan umum pada jaringan Wi-Fi dan cara mengatasi masalah keamanan yang muncul.

Dalam penelitian yang dilakukan (Saraun et al., 2022) berjudul "Analisa Keamanan Jaringan Nirkabel IEEE 802.11 pada Kantor Dinas Pendidikan Kabupaten Minahasa" Tujuan dari penelitian ini adalah untuk menganalisis sistem keamanan jaringan di Dinas Pendidikan Kabupaten Minahasa. Tes untuk *cracking the encryption, ARP poisoning* dan *denial of service* pada jaringan nirkabel. Penelitian ini menggunakan metode pengujian penetrasi. Serangan terhadap jaringan nirkabel berhasil karena sistem keamanan yang diterapkan Dinas Pendidikan Minahasa masih belum cukup aman. Hasil penelitian ini dapat digunakan oleh pengelola jaringan sebagai bahan untuk memperbaiki atau meningkatkan sistem keamanan jaringan Dinas Pendidikan Minahasa.