BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi jaringan komputer memudahkan orang untuk memenuhi kebutuhan informasi. Salah satu teknologi yang berkembang pesat adalah teknologi media transmisi nirkabel atau *wireless.* Media transmisi yang digunakan *wireless* adalah gelombang radio yang dipancarkan kesemua area yang bisa dijangkau oleh gelombang radio tersebut.(sabdho & ulfa, 2018).

Beberapa vendor menyediakan fitur-fitur yang memudahkan pengguna maupun administrator jaringan untuk menggunakannya, sehingga sering dijumpai masih menggunakan konfigurasi *default* dari vendor. Oleh karena itu, para *hacker* sering melakukan aksi untuk menguji kemampuan yang telah di pelajari sebelumnya. Kemudian terhubung dalam satu jaringan yang sama dan mengambil data pengguna lainnya secara ilegal.(Pratama & Syamsuar, 2021)

Pada saat para *hacker* melancarkan aksinya ditempat umum seperti kafe, *public hostpot* dan restoran. Karena sebagian pengguna tidak peduli dengan keamanan komunikasi data di tempat publik, maka tempat *hacker* untuk melakukan uji coba ilegal melalui jaringan *wireless* yang terhubung ke *hacker*. Jika dibandingkan dengan jaringan kabel. Jaringan *wireless* lebih rentan dan mudah masuk kedalam jaringan *wireless* yang tersedia. Cukup mendapatkan *password wifi* sudah bisa terhubung ke jaringan yang dituju oleh *hacker*(Haeruddin & Kurniadi, 2021)

Penerapan keamanan jaringan nirkabel sebagai bagian dari sistem menjadi peningkatan untuk menjaga keamananan data dan integritas. Keamanan jaringan nirkabel untuk perangkat AP (*Access Point*) Metode keamanan umum adalah WEP *(Wired Equivalent Privacy),* WPA *(WI-FI Protected Access*), dan WPA2 *(WI-FI Protected Access 2*), yang merupakan jaringan nirkabel. Hampir semua pengguna.

Rata-rata penggunaan perangkat AP menggunakan metode standar pabrikan (Hermanto & Anam, 2020).

Kali Linux (*Kali*) adalah sistem operasi distribusi *Linux* yang dikembangkan dengan fokus pada tugas pengujian penetrasi. *Kali Linux* sebelumnya dikenal sebagai *BackTrack*. Untuk mengintegrasikan tiga distribusi pengujian penetrasi *Linux* yang berbeda: *IWHAX, WHOPPIX*, dan *Auditor*. *BackTrack* adalah salah satu sistem distribusi *Linux* paling populer, terbukti dengan jumlah unduhan melebihi 4 juta di *BackTrack Linux* 4.0 pra-final *Linux*(Santoso. 2022)

Tahap pengujian akan di lakukan pada *access point* Tp-link WA701ND, Tenda F3 dan *Hotspot Smartphone* Realmi 5i. Tahap pengujian diawali dengan melakukan *Network mapping* yaitu mengumpulkan data-data yang diperlukan sebelum melakukan *penetration testing* pada jaringan nirkabel pada 3 perangkat tersebut, serta mengidentifikasi sistem keamanan yanga ada pada perangkat *acces point* dan *hotspot smartpone*. Penggunaan *tools* akan dilakukan saat proses pengujian ini sehingga mempermudah dalam pengujian. Sistem operasi yang digunakan dalam pengujian ini yaitu sistem operasi *kali linux*.

Access point merek Tp-link WA701ND dan Tenda F3 yang umum orang gunakan dalam pemasangan wifi. Yang masih menggunakan sistem keamanan WPA2-PSK.

1.2 Perumusan Masalah

Ada beberapa rumusan masalah antara lain :

1. Bagaimana menerapkan teknik *penetration testing* dijaringan *wireless*.?
2. Bagaimana cara pengujian jaringan nirkabel WPA2-PSK dengan metode *penetration testing* .?
3. Bagaimana cara meminimalisir WPA2-PSK mengalami serangan?

1.3 Batasan Masalah

Ada beberapa batasan masalah antara lain:

1. Menerapkan pengujian keamanan jaringan nirkabel WPA2-PSK pada *access point* Tp-link WA701ND, Tenda F3 dan *Hotspot Smartphone* Realmi 5i dengan motode *penetration testing*
2. Penyerangan sistem menggunakan sistem operasi *kali linux* dan menggunakan *tools airmon-ng, airodump-ng, aireplay-ng, aircrack-ng.*
3. Ruang lingkup pengujian jaringan nirkabel WPA2-PSK pada *access point* Tp-link WA701ND, Tenda F3 dan *Hotspot Handphone* Realmi 5i

1.4 Tujuan dan Manfaat

Adapun tujuan dan manfaat dari Tugas Akhir ini adalah:

1.4.1 Tujuan

Beberapa tujuan dalam penelitian ini :

1. Menguji keamanan jaringan nirkabel WPA2-PSK yang ada pada *access point* Tp-link WA701ND, Tenda F3 dan *Hotspot Smartphone* dengan metode *penetration testing*.
2. Melakukan penyerangan pada WPA2-PSK dengan menggunakan sistem operasi *kali linux.*
3. Melakukan peningkatan keamanan pada jaringan nirkabel WPA2-PSK.

1.4.2 Manfaat

Manfaat dari penelitian ini :

1. Mengetahui celah keamanan yang ada di WPA2-PSK pada jaringan nirkabel.
2. Mendapatkan peningkatan keamanan pada WPA2-PSK.
3. Memperkuat keamanan WPA2-PSK di jaringan nirkabel pada tipe perangkat access point Tp-link WA701ND, Tenda F3 dan Hotspot Smartphone.

1.5 Metode Penyelesaian Masalah

Metode penyelesaian masalah dalam Pengujian Keamanan Jaringan Nirkabel(WPA2-PSK) Menggunakan Metode *Penetration Testing*

1. Melakukan analisa pada *Access Point* untuk melihat keamanan yang sudah ada pada *Access Point* tersebut.
2. Melakukan penyerangan serta melakukan pengamanan tingkat lanjut kepada *Access Point* setelah dilakukan penyerangan.
3. Pengumpulan data yang akan dilakukan setelah melakukan penyerangan pada *Access point*. Data tersebut berguna sebagai acuan dalam pengujian. Pengumpulan data dilakukan melalui *scanning* bssid.
4. Selanjutnya pengujian sistem *Access Point* yang bertujuan untuk mengetahui cara kerja sebuah *Access Point* serta celah keamanan, sehingga memudahkan dalam penyerangan.