BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Saat ini perkembangan teknologi informasi sudah sangat pesat, khususnya pada koneksi internet berbasis jaringan nirkabel. Bentuk layanan jaringan nirkabel terimplementasi di banyak tempat seperti Bandara, Hotel, Sekolah, dan Kafe. Perangkat yang mendukung jaringan nirkabel seperti *Smartphone*, Laptop/Komputer (Rinaldi & Sadikin, 2019). Universitas Jenderal Achmad Yani Yogyakarta telah menggunakan teknologi jaringan untuk mendukung semua aktivitas perkulihan secara *online* maupun *offline* juga melakukan pelayanan pemrosesan informasi yang menggunakan jaringan nirkabel untuk membagi semua informasi tersebut. Namun, saat berbagi data melalui jaringan nirkabel, masih terdapat kerentanan dalam mengakses jaringan yang dapat diakses secara ilegal oleh peretas dan masih adanya, kekurangan dalam tingkat kesadaran Mahasiswa Universitas Jenderal Achmad Yani Yogyakarta tentang mewaspadai ancaman/serangan pada jaringan nirkabel sehingga Mahasiswa dengan tanpa sadar menghubungkan perangkatnya ke jaringan nirkabel secara bebas dan tidak mengetahui bahwa terdapat *Access Point* palsu di jaringan nirkabel. Salah satu contoh serangan jaringan nirkabel adalah serangan *Evil Twin*, serangan ini dapat dibedakan menjadi dua jenis, yaitu serangan *active attack* dan *passiive attack*, perbedaan serang ini adalah pengguna mengetahui atau tidak. Contoh serangan *active attack* terdiri dari *Hijacking, Denial of Service* dan sebaginya, sedangkan *passive attack* serangan dilakukan melalui *Rouge Access Point* (Utama et al., 2020).

Serangan *Evil Twin* dengan *Rouge Acces Point* merupakan serangan yang berbahaya karena peretas sering mengelabui pengguna dengan membuat *Access Point* palsu agar pengguna menyambungkan perangkatnya sehingga pengguna mengakses sesuatu di jaringan nirkabel agar peretas mengetahui aktivtas pengguna dalam menggunakan internet (Syahrulah et al., 2018). Dalam serangan yang

ditujukan ke *access point* menggunakan *Hijacking* dengan teknik MITM *(Man In The Middle)* yang menyerang jaringan nirkabel sehingga berdampak pencurian atau modifikasi informasi pengguna. *Hijacking* adalah serangan keamanan terhadap jaringan nirkabel yang melalui server *DNS* dan *Klien* serta dapat mengirimkan data palsu yang sudah dicuri kepada klien (Purba & Amri, 2023). Hal ini terjadi karena jaringan nirkabel menyediakan layanan seperti *SSID, IP Address, Remote Management, DHCP Enable*, Saluran Frekuensi secara *default* yang tidak menggunakan metode keamanan seperti WEP *(Wired Equivalent Privacy*) dan WPA (*Wi-Fi Protected Access*), yang menjadi standar keamanan jaringan nirkabel sebelumnya (Darma et al., 2023)**.** Dalam keamanan jaringan nirkabel terdapat perkembangan dalam keamananya seperti WPA, WPA2, WPA3, WPA Enterprise, No Encryption yang memiliki keunggulan tersendiri. WPA adalah sistem keamanan yang mengenkripsi lalu lintas jaringan 128-bit dengan kunci 256-bit bersama, WPA2 adalah sistem keamanan yang menggunakan AES (*Advanced Encryption Standard*) dan menggunakan kunci otentikasi yang lebih aman dari pada WPA, WPA3 adalah sistem keamanan yang menggukan pengaturan di antarmuka pengguna (UI) dalam browser lokal, WPA Enterprise adalah jenis keamanan jaringan tingkat lanjut yang menggunakan otentikasi dan enkripsi tingkat lanjut untuk perusahaan kecil atau besar, No Encryption adalah keamanan jaringan nirkabel yang paling retang di serang karena tidak menerapkan otentikas (Purweni et al., 2022).

Oleh karena itu, untuk memiliki jaringan nirkabel yang sepenuhnya aman, harus memperhatikan *access point* dengan memeriksa pengaturan jaringan nirkabel secara rutin (Ilman Zuhri Yadi, n.d.)**.** Mengingat pentingnya keamanan jaringan nirkabel di era komunikasi digital saat ini, sangat rentan terhadap serangan peretas yang merugikan penggunanya (Nugraha, 2021). Selain itu, Indonesia adalah negara yang mudah rentan di serang oleh peretas (Prakasa, 2020). Maka perlu dilakukan edukasi kepada masyarakat tentang perlunya kesadaran dan kewaspadaan terhadap serangan jaringan nirkabel. Pada penelitian ini penulis mengusulkan analisis serangan *Evil Tw*in pada suatu lokasi untuk mengetahui *access point* palsu yang

digunakan untuk pencurian informasi. Lokasi yang dijadikan obyek penelitian adalah Kampus Unit 1 Universitas Jenderal Achmad Yani Yogyakarta.

1.2 PERUMUSAN MASALAH

Berdasarkan latar belakang di atas bahwa permasalahan yang terjadi karena tingkat kesadaran Mahasiswa Universitas Jenderal Achmad Yani Yogyakarta masih kurang dalam mewaspadai ancaman/serangan pada jaringan nirkabel sehingga secara tidak sadar Mahasiswa menghubungkan perngkatnya ke jaringan nirkabel secara bebas dan tidak mengetahui bahwa adanya *Access Point* Palsu di jaringan nirkabel pada Gedung Universitas Jenderal Achmad Yani Yogyakarta Unit 1 yang disiapkan oleh peretas.

1.3 PERTANYAAN PENELITIAN

Berikut ini pertanyaan-pertanyaan yang menjadi dasar dalam penelitian serangan *Evil Twin*, yaitu:

1. Dimana lokasi serangan *Evil Twin*?
2. Siapa target dalam serangan *Evil Twin*?
3. Kapan serangan *Evil Twin* akan dilakukan?
4. Mengapa serangan *Evil Twin* harus dicegah?
5. Bagaimana proses simulasi serangan *Evil Twin*?
6. Bagaimana dampak yang akan ditimbulkan?

1.4 TUJUAN PENELITIAN

Tujuan dari penelitian ini untuk mengetahui dampak negatif yang berbahaya dari serangan *Evil Twin* kepada pengguna yang terhubung jaringan nirkabel. Adapun tujuan penelitian ini sebagai berikut:

1. Memberikan Edukasi dengan menggunakan Poster sebagai tempat informasi.
2. Untuk menganalisis dan menguji keamanan jaringan nirkabel
3. Merumuskan solusi dalam penanganan serang *Evil Twin* pada jaringan nirkabel.

1.5 MANFAAT HASIL PENELITIAN

Dalam manfaat penelitian ini memberikan wawasan kepada pengguna untuk lebih waspada ketika terhubung dengan jaringan nirkabel sehingga dapat mencegah serangan *Evil Twin* yang berdampak pada pencurian informasi data pengguna. Oleh sebab itu penelitian ini diharapkan dapat memberikan manfaat kepada pengguna diantaranya:

1. Memberikan wawasan cara membedakan *Access Point* palsu dan benar.
2. Memberi kewaspadaan tentang kerentanan jaringan nirkabel
3. Memberikan informasi tentang pola serangan *Evil Twin*
4. Memberikan edukasi kepada masyarakat tentang serangan *Evil Twin*