BAB I PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi informasi telah memacu munculnya inovasi dalam layanan perbankan, salah satunya *Internet banking*. Layanan ini memudahkan nasabah dalam mengakses dan melakukan transaksi perbankan secara online. Namun, kemudahan ini juga membawa potensi risiko terhadap keamanan data pribadi dan transaksi nasabah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Salah satu ancaman terbaru yang mulai berkembang adalah *Quishing* atau *Quick Response* (QR) *Code Phishing*. *Quishing attack* merupakan jenis serangan *phishing* yang menggunakan QR *Code* untuk menipu korban agar mengakses *website* berbahaya atau mengunduh *malware* tanpa disadari (Vaithilingam & Shankar, 2024).

Dalam penelitian yang dilakukan oleh Blanker (2024) dipublikasikan oleh Barracuda, dijelaskan bahwa dalam periode Juni 2024 sampai dengan September 2024, ditemukan 562.085 serangan *phishing email* menggunakan QR *Code* yang disisipkan dalam dokumen pdf. Data ini menunjukkan peningkatan signifikan dalam jumlah serangan berbasis QR *Code* yang terdeteksi. Meskipun serangan *phishing* melalui QR *Code* lebih sering terjadi melalui *email* namun serangan ini dapat terjadi pada berbagai *platform* komunikasi lainnya.

Quishing attack sering diabaikan padahal serangan ini memiliki potensi besar untuk merugikan korban, terutama dalam *Internet banking*. Banyak pengguna tidak menyadari bahwa dengan *scan* QR *Code* berbahaya dapat menyebabkan data pribadi terungkap dan disalahgunakan sehingga menimbulkan kerugian finansial (Bekavac dkk., 2024). Data publik yang tersedia seperti yang dimiliki oleh Bank XYZ dapat meningkatkan potensi risiko ini. Informasi yang terbuka untuk umum seperti informasi layanan dan kontak bank dapat dimanfaatkan untuk melakukan *social engineering.* Salah satu langkahnya adalah pembuatan *cloned website* yang menyerupai *website* resmi Bank XYZ, di mana nasabah diarahkan untuk memasukkan data sensitif ke dalam *website* tersebut.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis keamanan informasi melalui percobaan pengujian *quishing attack.* Pengujian ini menggabungkan serangan OSINT, *social engineering* dan QR *Code*. Serangan *Open-Source Intelligence* (OSINT) memungkinkan pengumpulan informasi dari berbagai sumber terbuka secara bebas dan mudah (Fadhli, 2024). Selain itu, memanfaatkan serangan *social engineering* untuk membuat *cloned website* dan *phishing* URL yang kemudian diubah menjadi QR *Code*. QR *Code* yang dihasilkan akan digunakan untuk menipu korban dengan mengarahkan ke *cloned website*. Informasi data yang diperoleh dari percobaan serangan akan diproses dan dianalisis untuk mengukur berdasarkan metrik pada *atttack tree diagram* dari *threat modeling quishing attack*. *Attack tree* merupakan metode yang digunakan untuk memetakan keamanan sistem dengan mengidentifikasi potensi-potensi serangan yang mungkin terjadi. Analisis ini dilakukan dengan membandingkan data hasil pengujian *quishing attack* sesuai metrik yang diukur dalam proses serangan tersebut. Tujuan dari hasil analisis ini ialah untuk memahami karakteristik *threat modeling* berdasarkan metrik yang digunakan pada *attack tree.*

I.2 Perumusan Masalah

Berdasarkan latar belakang permasalahan di atas, maka rumusan masalah yang mendasari penelitian ini adalah:

a. Bagaimana cara mengenali mekanisme *quishing attack* sebagai dasar perancangan *threat modeling* menggunakan kombinasi serangan OSINT, *social engineering* dan QR *Code*?
b. Bagaimana cara menganalisis dan mengidentifikasi *attack tree* yang berbeda berdasarkan kombinasi serangan dalam *quishing attack* menggunakan suatu metrik?
c. Bagaimana cara membandingkan perbedaan karakteristik hasil tiap serangan OSINT, *social engineering*, dan QR *Code* dalam *attack tree*?

I.3 Tujuan Penelitian

Sesuai dengan permasalahan yang telah dirumuskan dan diajukan di atas, maka tujuan dari penelitian ini yaitu sebagai berikut:

a. Merancang dan menganalisis *threat modeling* dari *quishing attack* menggunakan kombinasi serangan yang berbeda.
b. Menganalisis dan mengidentifikasi jumlah langkah pada *attack tree* yang berbeda berdasarkan kombinasi serangan dalam *quishing attack* dengan menggunakan metrik cost.
c. Menganalisis dan membandingkan perbedaan karakteristik hasil tiap serangan pada *attack tree*.

I.4 Batasan Penelitian

Adapun batasan penelitian pada penelitian ini adalah sebagai berikut:

a. Pengujian *quishing attack* hanya sebatas *Proof of Concept* (PoC) tidak dilanjutkan sampai ke tahap *attack launching* atau eksploitasi secara nyata.
b. Penelitian ini hanya fokus pada analisa *attack tree* berdasarkan *quishing attack*, tanpa membahas aspek kerentanan dan mitigasi serangan.
c. Analisis karakteristik *attack tree* hanya berfokus pada metrik *cost* yang dibandingkan secara kuantitatif.

I.5 Manfaat Penelitian

Adapun manfaat yang didapatkan dengan adanya penelitian Tugas Akhir ini adalah sebagai berikut:

1. Secara teoritis
   a. Menambah wawasan terhadap *quishing attack* menggunakan serangan OSINT, *social engineering* dan QR *Code* berdasarkan pada penyusunan *attack tree*.
   b. Dapat mengetahui karakteristik *attack tree* berdasarkan metrik *cost*.
2. Secara praktis
   a. Memahami mekanisme serta cara kerja *quishing attack*, sekaligus memahami tahapan ancamannya.
   b. Mampu mengenali dan menggunakan *software open source* untuk serangan OSINT, *social engineering*, dan QR *Code*.

I.6 Sistematika Penulisan

Sistematika penulisan Tugas Akhir ini terdiri dari enam bab, antara lain:

Bab I Pendahuluan

Bab ini menjelaskan rumusan masalah mengenai bagaimana cara mengenali mekanisme *quishing attack* sebagai dasar perancangan *threat modeling* menggunakan kombinasi serangan OSINT, *social engineering* dan QR *Code*, mengidentifikasi salah satu karakteristik *attack tree*, dan membandingkan *attack tree* yang berbeda berdasarkan kombinasi serangan dalam *quishing attack* menggunakan suatu metrik. Tujuan penelitian ini yaitu merancang dan menganalisis *threat modeling* dari *quishing attack* menggunakan kombinasi serangan yang berbeda, menganalisis dan mengidentifikasi metrik *cost* pada *attack tree* untuk setiap serangan, serta menganalisis jumlah langkah yang didapatkan dari *attack tree* yang berbeda menggunakan metrik *cost*. Batasan penelitian ini yaitu hanya sebatas *Proof of Concept* (PoC), hanya fokus pada analisa *attack tree* berdasarkan *quishing attack* tanpa membahas aspek kerentanan dan mitigasi serangan, serta analisis karakteristik *attack tree* hanya berfokus pada metrik *cost* yang dibandingkan secara kuantitatif. Penelitian ini juga memiliki manfaat secara teoritis dan secara praktis.

Bab II Tinjauan Pustaka

Bab ini menjelaskan teori-teori pendukung dari permasalahan yang akan diteliti, seperti data publik, *open-source intelligence, threat, cyber security, social engineering, phishing attack, quishing attack*, QR *Code*, metrik *cost, threat modeling, attack tree, flowchart diagram* dan *data flow diagram* serta penelitian-penelitian serupa yang berkaitan dengan topik yang akan diteliti.

Bab III Metodologi Penelitian

Bab ini menjelaskan metode konseptual yang terdiri dari Lingkungan, Penelitian dan Dasar Ilmu. Lingkungan terdiri dari Pengguna, Organisasi dan Teknologi. Pengguna mengungkapkan kemungkinan terjadinya *quishing attack* pada layanan *Internet banking* dengan

serangan OSINT, *social engineering*, dan QR *Code* serta metrik *cost*. Organisasi pada penelitian ini berfokus pada Bank XYZ. Teknologi dalam penelitian ini yaitu OSINT, *social engineering*, dan QR *Code*. Penelitian terdiri dari Merancang dan Evaluasi. Merancang digunakan untuk menggambarkan *attack tree* berdasarkan pada proses *quishing attack*. Evaluasi menjelaskan mengenai eksperimen serangan OSINT, *social engineering*, dan QR *Code*, analisis eksperimen *quishing attack*, serta analisis *attack tree* dan metrik *cost*. Dasar Ilmu terdiri dari Dasar Teori dan Metode. Dasar Teori yang digunakan adalah teori *quishing attack*, *social engineering*, OSINT, *attack tree*, dan metrik *cost*. Metode yang digunakan adalah studi literatur, *attack tree*, dan metrik *cost*. Bab ini juga menjelaskan sistematika penyelesaian masalah yang terdiri dari enam tahap. Tahap awal yaitu bagaimana merancang *threat modeling* dari *quishing attack* berdasarkan data publik. Tahap hipotesis yaitu perkiraan awal mengenai *attack tree* berdasarkan serangan OSINT, *social engineering* dan QR *Code* yang menghasilkan *quishing attack*. Tahap desain yaitu merancang alur eksperimen untuk masing-masing serangan. Tahap eksperimen yaitu implementasi dari desain yang telah dirumuskan sebelumnya. Tahap analisis yaitu pengumpulan data dari masing-masing serangan yang kemudian dianalisis untuk menyusun *attack tree* dari *quishing attack* dan dikategorikan berdasarkan metrik *cost*. Tahap akhir yaitu penyusunan laporan berdasarkan hasil analisis dan eksperimen. Bab ini juga menjelaskan proses pengolahan data dari hasil pengumpulan eksperimen dan perbandingan karakteristik *attack tree* berdasarkan metrik *cost*.

Bab IV Perancangan dan Alur Eksperimen

Bab ini menjelaskan tahapan eksperimen yang dimulai dari perencanaan dan persiapan eksperimen yang terdiri dari spesifikasi perangkat keras dan perangkat lunak yang digunakan, daftar IP *address*, *platform* eksperimen, alur eksperimen, implementasi eksperimen, dan data hasil eksperimen dari serangan OSINT, *social*

engineering, QR *Code* berdasarkan konten pesan *phishing* di WhatsApp.

Bab V **Analisis**

Bab ini menjelaskan hasil analisis serangan OSINT, *social engineering*, dan QR *Code* melalui konten pesan *phishing* di WhatsApp, analisis data serangan, penyusunan kombinasi serangan yang menghasilkan *quishing attack*, penyusunan *attack tree*, dan pemeringkatan berdasarkan metrik *cost*. Pada bab ini juga dijelaskan hasil analisis dari perbandingan kombinasi *quishing attack* berdasarkan metrik *cost* dan terdapat ringkasan analisis.

Bab VI **Kesimpulan dan Saran**

Bab ini menjelaskan kesimpulan dari hasil eksperimen yang didapatkan yaitu relasi antara kombinasi serangan OSINT, *social engineering*, dan QR *Code* melalui konten pesan *phishing* di WhatsApp. Berdasarkan kerangka *Proof of Concept* (PoC), kombinasi serangan tersebut dianalisis untuk menghasilkan *attack tree diagram* yang merepresentasikan langkah-langkah dan mekanisme untuk mencapai tujuan serangan.