BAB I PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi informasi telah memberikan dampak terhadap berbagai aspek kehidupan manusia, khususnya pada sektor keuangan atau perbankan. *Internet banking* menjadi salah satu layanan perbankan yang memudahkan nasabah dalam melakukan transaksi secara *online*. Namun, perkembangan ini menimbulkan tantangan baru dengan munculnya berbagai *cybercrime* oleh pihak-pihak yang berusaha memanfaatkan kelemahan sistem (Muftiadi dkk., 2022). Salah satu bentuk *cybercrime* yang sangat umum digunakan adalah *phishing,* yang bertujuan untuk mengelabui target untuk membagikan informasi sensitif seperti kredensial akun, detail pribadi, informasi kartu kredit dan akun keuangan, dll (Rains, 2020). Serangan ini dilakukan menggunakan teknik *social engineering,* yang memanfaatkan kelemahan target agar dapat memperoleh informasi, akses, dan mendorong target untuk melakukan tindakan tertentu (Hidayah, 2020). Berdasarkan laporan *Indonesia Domain Abuse Data Exchange*, kategori serangan yang paling banyak dilaporkan adalah *phishing*, dengan total sebanyak 85.414 laporan (IDADX, 2024) .

Insiden *phishing* marak terjadi pada layanan perbankan *online* di bank-bank di Indonesia (Pranata & Ependi, 2023). Serangan *phishing* dapat terus meningkat dan menjadi ancaman serius pada sektor perbankan. Dampak dari serangan ini mencakup kerugian finansial, mengakibatkan kebocoran data sensitif nasabah, serta penurunan reputasi yang dapat menurunkan kepercayaan nasabah terhadap keamanan dan integritas layanan perbankan (Wibowo & Hidayat, 2024). Salah satu kasus *phishing* di Bank BRI terjadi pada tahun Mei 2023, di mana nasabah tersebut menjadi korban *phishing* setelah menerima pesan berisi undangan dengan format apk. Setelah dibuka, terdapat iklan yang muncul dan pengurangan saldo rekening sebesar Rp 1,4 miliar dalam waktu singkat (Rahmadian dkk., 2021). Insiden ini menunjukkan bagaimana pelaku memanfaatkan data publik, termasuk informasi perbankan dan data pribadi korban, seperti nomor telepon.

Saat ini, terdapat jenis *cybercrime* terbaru yang dikenal sebagai *quishing.* Serangan ini menggabungkan teknik *phishing* dengan teknologi *Quick Response* (QR) *Code* untuk mencuri informasi pengguna (Fridayani & Cuaca, 2023). *Quick Response* (QR) *Code* diciptakan pada tahun 1994 untuk kebutuhan industri otomotif. Sejak tahun 2010, QR *Code* mulai berkembang luas di China seiring dengan fitur *scan Quick Response* (QR) *Code* yang terintegrasi pada kamera ponsel dan berkembang menjadi alat untuk pembayaran digital (Greenspan, 2021). Seiring dengan berkembangnya penggunaan *Quick Response* (QR) *Code,* pelaku kejahatan memanfaatkan celah keamanan untuk melakukan *phishing attack* berbasis *Quick Response* (QR) *Code* atau *quishing*. Hal ini terlihat dengan meningkatnya *quishing attack* sebesar 51% di bulan September 2023 dibandingkan delapan bulan sebelumnya (ReliaQuest, 2023). Dalam *quishing attack*, *Quick Response* (QR) *Code* disisipkan untuk menipu pengguna dengan mengarahkan pengguna ke situs web atau aplikasi berbahaya agar memperoleh informasi sensitif.

Untuk menganalisis *quishing attack*, diperlukan pendekatan *threat modeling* yang terstruktur dengan menggunakan *attack tree*. *Attack tree* digunakan untuk memetakan berbagai skenario serangan. Setiap *node* pada *attack tree* menggambarkan langkah dalam melakukan serangan. Dengan mengintegrasikan metrik *time* pada setiap tahapan, durasi yang dibutuhkan untuk menyelesaikan setiap tahapan serangan dapat diukur, serta menganalisis efisiensi waktu pada setiap tahapan. Metrik *time* juga memungkinkan untuk menentukan langkah-langkah yang membutuhkan waktu lebih cepat untuk mencapai tujuan serangan.

Oleh karena itu, diperlukan pengujian keamanan untuk melindungi data di instansi publik perbankan. Penelitian ini dilakukan dengan studi kasus *Internet banking* Bank ABC, dengan melakukan percobaan pengujian terhadap salah satu jenis *phishing*, yaitu *quishing attack* yang memanfaatkan data publik sebagai target. Dengan menggunakan metode *Open Source Intelligence* (OSINT) untuk menemukan kerentanan dengan mendapatkan data publik (Pratiwi dkk., 2024). Selain itu, memanfaatkan serangan *social engineering* untuk memanipulasi target melalui *Quick Response* (QR) *Code* yang dirancang sedemikian rupa sehingga terlihat sah. *Quick Response* (QR) *Code* yang diimplementasikan akan berperan sebagai penghubung untuk mengarahkan target ke situs web palsu yang dibuat seolah-olah merupakan *Internet banking* milik Bank ABC.

I.2 Perumusan Masalah

Rumusan masalah yang mendasari penelitian ini adalah:

a. Bagaimana cara menyusun *threat modeling* pada *quishing attack* dengan berbagai macam serangan?
b. Bagaimana mengidentifikasi karakteristik *quishing attack* dari beberapa *attack tree* menggunakan metrik tertentu?
c. Bagaimana membandingkan karakteristik dari berbagai serangan dalam *attack tree*?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

a. Menyusun dan menganalisis *quishing attack* dari kombinasi serangan OSINT, *social engineering*, dan QR *Code*.
b. Menganalisis dan mengidentifikasi durasi waktu pada setiap *attack tree* dalam *quishing attack* menggunakan metrik *time*.
c. Menganalisis perbedaan karakteristik serangan OSINT, *social engineering*, dan QR *Code* pada setiap *attack tree*.

I.4 Batasan Penelitian

Adapun batasan penelitian ini adalah:

a. Penelitian ini hanya berfokus pada pengujian dan implementasi *quishing attack* atau terbatas *Proof of Concept* (PoC), tidak sampai pada tahap eksploitasi.
b. Pembahasan perbandingan *time* pada *attack tree* dari *quishing attack* menggunakan ketegori *real time*.
c. Penelitian ini terbatas pada analisis *attack tree*, tanpa membahas aspek kerentanan dan mitigasi serangan.

I.5 Manfaat Penelitian

Manfaat penelitian ini adalah:

1. Secara teoritis
   a. Dapat menambah pengetahuan mengenai *quishing attack* melalui kombinasi serangan OSINT, *social engineering*, dan QR *Code* berdasarkan penyusunan *attack tree*.

   b. Dapat mengenali karakter *attack tree* berdasarkan metrik *time*.
2. Secara praktis
   a. Memahami ancaman keamanan dari *quishing attack* melalui langkah-langkah dalam proses serangan.
   b. Mengetahui penggunaan *software open-source* untuk serangan OSINT, *social engineering*, QR *Code* pada *quishing attack*.

I.6 Sistematika Penulisan

Penelitian ini diuraikan dengan sistematika penulisan sebagai berikut:

Bab I **Pendahuluan**

Pada bab ini berisi uraian perumusan masalah terkait menyusun *threat modeling* pada *quishing attack*, mengidentifikasi karakteristik dari beberapa *attack tree*, membandingkan *attack tree* pada *quishing attack* berdasarkan metrik *time* berdasarkan kombinasi serangan OSINT, *social engineering*, dan QR *Code*. Bab ini juga menguraikan tujuan penelitian menyusun *quishing attack* dari berbagai macam serangan, menganalisis dan mengidentifikasi metrik *time* pada *attack tree*, serta menganalisis perbandingan penggunaan metrik *time*. Batasan penelitian ini adalah berfokus pada pengujian dan implementasi *quishing attack* atau terbatas *Proof of Concept* (PoC), analisis *attack tree* tanpa membahas aspek kerentanan dan mitigasi serangan, serta perbandingan metrik *time* menggunakan ketegori *real time*. Penelitian ini juga memiliki manfaat secara teoritis dan praktis.

Bab II **Tinjauan Pustaka**

Bab ini berisi literatur yang relevan dengan permasalahan yang diteliti seperti *Internet banking*, *cybercrime*, *phishing attack*, *social engineering*, *threats*, OSINT, QR *Code*, *quishing attack*, *threat modeling*, *attack tree*, metrik *time*, *flowchart diagram*, dan *Data Flow Diagram* (DFD). Bab ini juga menguraikan hasil penelitian terdahulu yang relevan dengan penelitian ini, yang dapat memperluas pemahaman terhadap topik yang sedang diteliti. Selain itu, bab ini menjelaskan alasan pemilihan kerja yang digunakan dalam penelitian.

Bab III **Metodologi Penelitian**

Bab ini menjelaskan metodologi penelitian melalui model konseptual yang terdiri komponen, yaitu Lingkungan, Penelitian, dan Teori Dasar. Bagian lingkungan berisi rendahnya kesadaran pengguna terhadap *quishing attack* pada layanan *Internet banking* di Bank ABC dengan penggunaan teknologi OSINT, *social engineering*, dan QR *Code.* Pada bagian penelitian berisi perancangan analisis metrik *time* dan evaluasi melalui eksperimen. Bagian teori dasar berisikan landasan konsep serta metodologi yang digunakan dalam penelitian. Pada bab ini juga dijelaskan sistematika penyelesaian masalah yang meliputi 6 tahap, yaitu tahap awal, tahap hipotesis, tahap desain, tahap eksperimen, tahap analisis, dan tahap akhir. Selain itu, bab ini berisi penjelasan mengenai pengumpulan data, pengolahan data, metode evaluasi, hingga alasan pemilihan metode.

Bab IV **Analisis dan Perancangan**

Pada bab ini dijelaskan tahapan dari perencanaan dan persiapan untuk melakukan eksperimen berupa spesifikasi perangkat keras, perangkat lunak, *platform* eksperimen, dan IP *address* yang digunakan, serta alur eksperimen, implementasi eksperimen, dan data hasil eksperimen dari serangan OSINT, *social engineering*, dan QR *Code* berdasarkan konten palsu melalui WhatsApp.

Bab V **Analisis**

Pada bab ini berisi hasil perumusan serangan OSINT, *social engineering*, dan QR *Code* yang disebarkan melalui konten palsu di WhatsApp, serta analisis terhadap data serangan yang diperoleh. Bagian ini juga menjelaskan mengenai perumusan kombinasi serangan yang membentuk *quishing attack*, penyusunan *attack tree*, dan analisis *attack tree* berdasarkan metrik *time*. Selain itu, dijelaskan hasil analisis perbandingan kombinasi *quishing attack* berdasarkan metrik *time*, serta ringkasan keseluruhan analisis.

Bab VI Kesimpulan dan Saran

Pada bab ini berisi kesimpulan dari seluruh rangkaian kegiatan yang dilakukan mengenai hubungan antara eksperimen serangan OSINT, *social engineering*, dan QR *Code* yang hanya sebatas *Proof of Concept* (PoC) dalam menyusun *attack tree*, serta analisis *metrik time* untuk menilai efisiensi setiap kombinasi serangan. Bab ini juga memuat saran yang dapat dijadikan acuan atau masukan untuk penelitian selannjutnya.