ABSTRAK

Perkembangan teknologi informasi telah mempermudah layanan perbankan melalui *Internet banking* yang memungkinkan nasabah mengakses rekening dan melakukan transaksi secara online. Namun, kemudahan ini juga membuka potensi serangan berbasis *Quick Reponse* (QR) *Code* atau *Quishing*. *Quishing* adalah jenis *phishing* yang memanfaatkan QR *Code* untuk mengarahkan korban ke *website* berbahaya dengan tujuan pencurian data pribadi secara tersembunyi. Penelitian ini dilakukan untuk menganalisis *quishing attack* pada nasabah Bank XYZ melalui penyusunan *attack tree* berdasarkan *data flow diagram* menggunakan metrik *cost* dengan menggabungkan serangan OSINT, *social engineering* dan QR *Code*. Tahapan serangan tersebut menghasilkan dua *attack tree* berdasarkan *Proof of Concept* (PoC) untuk mendapatkan gambaran *attack launching* atau eksploitasi. Berdasarkan pengukuran *attack tree* menggunakan metrik *cost*, didapatkan hasil bahwa serangan dengan jumlah langkah paling sedikit dengan 26 *steps* adalah *quishing attack* dengan kombinasi serangan OSINT Truecaller, serangan *social engineering* SEToolkit, dan serangan QR *Code* qrencode melalui konten pesan *phishing* di WhatsApp. Hal ini menjadikannya sebagai *attack tree* dengan efektivitas serangan terbaik dan menempatkannya pada peringkat pertama. *Quishing attack* ke dua dengan jumlah langkah sebanyak 29 *steps* adalah *quishing attack* dengan kombinasi serangan OSINT Sync.ME, serangan *social engineering* SocialFish, dan serangan QR *Code* qrencode melalui konten pesan *phishing* di WhatsApp. Perbedaan utama pada kedua *attack tree* tersebut terletak pada tahapan serangan *social engineering* yang digunakan, sedangkan serangan OSINT dan serangan QR *Code* tidak terdapat perbedaan.

Kata kunci— ***social engineering, quishing, OSINT, attack tree, metrik cost***