ABSTRAK

Perkembangan teknologi pada layanan *Internet banking* memudahkan nasabah dalam melakukan transaksi keuangan. Namun, hal ini juga dapat menimbulkan peluang terhadap ancaman *cybercrime*, salah satunya adalah *quishing attack*. *Quishing attack* merupakan bentuk *phishing attack* yang memanfaatkan *Quick Response* (QR) *Code* untuk mengarahkan korban ke website palsu dengan tujuan mencuri informasi sensitif. Penelitian ini bertujuan untuk merumuskan *attack tree* pada *quishing attack* terhadap nasabah Bank ABC dengan kombinasi serangan OSINT, *social* engineering, dan *Quick Response* (QR) *Code* berdasarkan *data flow diagram*, serta mengurutkan hasil serangan dengan metrik *time*. Tahapan serangan dibatasi *Proof of Concept* (PoC) sebagai bentuk simulasi serangan yang memberikan gambaran nyata terkait ekploitasi dalam *quishing attack*. Hasil dari penelitian ini menunjukkan quishing attack dengan serangan tercepat adalah serangan OSINT Truecaller, *social engineering* SEToolkit, dan QR *Code* Qrencode sebesar 248,31 detik. Untuk posisi ke dua ditempati oleh serangan OSINT Find Mobile Number Location, *social engineering* SEToolkit, dan QR *Code* Qrencode sebesar 273,46 detik. Pada kedua *attack tree* yang telah disusun, serangan *social engineering* dan *Quick Response* (QR) *Code* memiliki peran yang serupa dalam menjalankan serangan. Untuk serangan OSINT, terdapat dua *tools* OSINT memiliki peran yang serupa dalam melakukan serangan, namun terdapat perbedaan durasi dalam proses serangan dengan selisih sebesar 25,15 detik. *Quishing attack* dengan penggunaan OSINT *tool* Truecaller dalam kombinasi serangan dianggap efisien, karena dapat melakukan pencarian dan pengumpulan data publik terkait nomor telepon dalam waktu 16,94 detik.

Kata kunci— ***attack tree*, metrik *time*, *quishing attack*, *social engineering***