# ABSTRAK

Pencarian dan pengumpulan data publik dapat dilakukan menggunakan *Open-Source Intelligence* (OSINT) yang memanfaatkan informasi dari sumber terbuka. Data publik ini dapat disalahgunakan untuk tujuan kriminal seperti pencurian identitas hingga menyebabkan kebocoran data. Pada bulan Mei tahun 2021, instansi ABZ mengalami kebocoran data lebih dari 80% warga Indonesia karena serangan siber. Salah satu serangan siber yang sering digunakan adalah *social engineering* yang memanipulasi individu untuk mengungkapkan data sensitif dan seringkali dilakukan melalui *phishing*. Serangan *phishing* yang menargetkan individu penting di organisasi dikenal sebagai *whaling attack*, yang biasanya dilakukan menggunakan *email* untuk menipu korban. Penelitian ini bertujuan merumuskan *attack tree* dari *whaling attack* yang menggabungkan serangan OSINT, *social engineering*, dan *email spoofing* berdasarkan *data flow diagram* yang diurutkan dengan metrik *time* atau waktu. Tahapan serangan tersebut menghasilkan tiga *attack tree*, namun tidak sampai ke tahap *attack launching* atau eksploitasi. Urutan pertama dan memiliki waktu paling cepat yaitu 144,32 detik adalah *whaling attack* dengan serangan OSINT Skymem, serangan *social engineering* Dark-Phish, dan serangan *email spoofing* Telnet. Kemudian, *whaling attack* yang berada pada urutan ke dua dengan waktu 200,01 adalah *whaling attack* dengan serangan OSINT Knockpy, serangan *social engineering* SEToolkit, dan serangan *email spoofing* Telnet. Terakhir, *whaling attack* yang berada pada urutan ke tiga dan memiliki waktu paling lama yaitu 795,33 detik adalah *whaling attack* dengan serangan OSINT SpiderFoot, serangan *social engineering* Dark-Phish, dan serangan *email spoofing* Telnet. *Whaling attack* menggunakan OSINT *tool* Skymem dalam kombinasi serangan dinilai paling efisien dalam mencari dan mengumpulkan data publik hanya dalam waktu 10,24 detik.

Kata kunci - ***attack tree, whaling attack,* OSINT, *social engineering, email spoofing*, metrik *time***