ABSTRAK

Keamanan data kini menjadi hal utama yang harus diperhatikan untuk melindungi data menyangkut informasi pribadi dan sensitif didalamnya. Kasus kebocoran data yang pernah terjadi di Indonesia tercatat bahwa 80% data warga Indonesia dijual di forum gelap (*dark web*), hal ini tentu akan menimbulkan kerugian bagi individu maupun organisasi. Faktor yang menjadi penyebab kebocoran data bisa dari kurangnya protokol keamanan, serangan langsung, ataupun *spear phishing attack*. Oleh karena itu, penelitian ini dilakukan untuk mengetahui potensi kebocoran data dari data publik instansi XYZ dengan merumuskan serangan *attack tree* berdasarkan *Data Flow Diagram* (DFD) dari *spear phishing attack* menggunakan metrik granularitas data dengan kombinasi serangan *Open Source Intelligence* (OSINT) *tools*, *social engineering tools*, dan *email spoofing*. Hasil dari penelitian ini merupakan perumusan empat model *attack tree* dari *spear phishing attack* yaitu kombinasi serangan OSINT TheHarvester, *social engineering* SEToolkit, dan *email spoofing*, kombinasi serangan OSINT Metagoofil, *social engineering* ZPhisher, dan *email spoofing*, kombinasi serangan OSINT Recon-ng, *social engineering* SEToolkit, dan *email spoofing*, serta kombinasi serangan OSINT Snov.io, *social engineering* ZPhisher, dan *email spoofing*. Setelah dilakukan percobaan dan analisis perbandingan model serangan *attack tree* dari *spear phishing attack* dengan metrik granularitas data dihasilkan bahwa kombinasi serangan OSINT Snov.io, *social engineering* ZPhisher, dan *email spoofing* mendapatkan lima jenis data dan jumlah data 367 merupakan kombinasi serangan terbaik dikarenakan memiliki rincian data yang bervariasi dan tingkat granularitas data yang tinggi sehingga semakin banyak peluang untuk melakukan perencanaan serangan dan analisis keamanan.

Kata kunci—***spear phishing attack, social engineering, OSINT, attack tree, metrik granularitas data***