ABSTRACT

Data security is now the main thing that must be considered to protect data regarding personal and sensitive information in it. Data leakage cases that have occurred in Indonesia have recorded that 80% of Indonesian citizen data is sold on dark forums (dark web), this will certainly cause losses for individuals and organizations. Factors that cause data leakage can be the lack of security protocols, direct attacks, or spear phishing attacks. Therefore, this research was conducted to determine the potential for data leakage from XYZ agency public data by formulating an attack tree based on the Data Flow Diagram (DFD) of a spear phishing attack using data granularity metrics with a combination of Open Source Intelligence (OSINT) tools, social engineering tools, and email spoofing attacks. The result of this research is the formulation of four attack tree models of spear phishing attacks, namely a combination of OSINT TheHarvester, social engineering SEToolkit, and email spoofing, a combination of OSINT Metagoofil, social engineering ZPhisher, and email spoofing, a combination of OSINT Recon-ng, social engineering SEToolkit, and email spoofing, and a combination of OSINT Snov.io, social engineering ZPhisher, and email spoofing. After the experiments and analysis of the comparison of attack tree models of spear phishing attacks with data granularity metrics, it was found that the combination of OSINT Snov.io, social engineering ZPhisher, and email spoofing with five types of data and a total of 367 data is the best attack combination because it has varied data details and a high level of data granularity so that there are more opportunities for attack planning and security analysis.

Keywords— ***spear phishing attack, social engineering, OSINT, attack tree, data granularity metrics***