ABSTRACT

Searching and collecting public data can be done using Open-Source Intelligence (OSINT) which utilizes information from open sources. This public data can be misused for criminal purposes such as identity theft to cause data leaks. In May 2021, ABZ instance experienced a data leak of more than 80% of Indonesians due to cyber attacks. One of the most commonly used cyberattacks is social engineering which manipulates individuals to reveal sensitive data and is often done through phishing. Phishing attacks that target important individuals in organizations are known as whaling attacks, which are usually carried out using email to deceive victims. This research aims to formulate the attack tree of a whaling attack that combines OSINT, social engineering, and email spoofing attacks based on a data flow diagram ordered by the time metric. The attack stages produced three attack trees, but did not reach the attack launching or exploitation stage. The first order and has the fastest time of 144.32 seconds is the whaling attack with OSINT Skymem attack, social engineerinh Dark-Phish attack, and email spoofing Telnet attack. Then, the whaling attack that is in second place with a time of 200.01 seconds is the whaling attack with OSINT Knockpy attack, social engineering SEToolkit attack, and email spoofing Telnet attack. Finally, the whaling attack that is in third place and has the longest time of 795.33 seconds is the whaling attack with OSINT SpiderFoot attack, social engineering Dark-Phish attack, and email spoofing Telnet attack. Whaling attacks using the OSINT tool Skymem in combination with attacks are considered the most efficient in searching and collecting public data in just 10.24 seconds.

Keywords - **attack tree, whaling attack, OSINT, social engineering, email spoofing, time metric**