ABSTRACT

The development of technology in Internet banking services makes it easier for customers to make financial transactions. However, this can also create opportunities for cybercrime threats, one of which is a quishing attack. A quishing attack is a type of phishing attack that uses Quick Response (QR) Code to direct victims to fake websites to steal sensitive information. This study aims to formulate an attack tree on a quishing attack against Bank ABC customers with a combination of OSINT, social engineering, and Quick Response (QR) Code attacks based on data flow diagrams, and to sort the attack results with time metrics. The attack stages are limited to Proof of Concept (PoC) as a form of attack simulation that provides a real picture of exploitation in a quishing attack. The results of this study show that the quishing attack with the fastest attack is the OSINT Truecaller attack, social engineering SEToolkit, and QR Code Qrencode of 248.31 seconds. The second position is occupied by the OSINT Find Mobile Number Location attack, social engineering SEToolkit, and Quick QR Code Qrencode of 273.46 seconds. In both attack trees that have been compiled, social engineering and Quick Response (QR) Code attacks have similar roles in carrying out attacks. For OSINT attacks, there are two OSINT tools that have a similar role in carrying out attacks, but there is a difference in duration in the attack process with a difference of 25.15 seconds. Quishing attacks using the Truecaller OSINT tool in a combination of attacks are considered efficient because they can search and collect public data related to telephone numbers in 16.94 seconds.

Keywords— ***attack tree*****, metrik** ***time*****, *quishing attack*****, *social engineering***