ABSTRACT

The development of information technology has facilitated banking services through Internet banking which allows customers to access accounts and conduct transactions online. However, this convenience also opens up the potential for Quick Response (QR) Code-based attacks or Quishing. Quishing is a type of phishing that utilized a QR Codes to direct victims to a malicious website with the aim of stealth theft of personal data. This research was conducted to analyze quishing attacks on Bank XYZ customers to the preparation of attack trees based on a data flow diagram using cost metrics by combining OSINT, social engineering, and QR Code attacks. The attack stages produce two attack trees based on Proof of Concept (PoC) to get an overview of attack launching or exploitation. Based on the measurement of the attack tree using the cost metric, the result show that the attack with the least number of steps with 26 steps is a quishing attack with a combination of OSINT Truecaller attacks, social engineering SEToolkit attacks, and QR Code qrencode attacks through phishing message content on WhatsApp. This makes it the attack tree with the best attack effectiveness and ranks it first. The second quishing attack with a total of 29 is a quishing attack with a combination of OSINT Sync.ME attacks, social engineering SocialFish attacks, and QR Code attacks through phishing message content on WhatsApp. The main difference between the two attack trees lies in the stages of social engineering attacks used, while the OSINT attacks and QR Code attacks have no difference.

Keywords— ***social engineering, quishing, OSINT, attack tree, cost metrics***