Analisis Metode Penyerangan dan Eksploitasi Web Browser dengan Menggunakan Browser Exploitation Framework (BeEF) Serta Langkah-langkah dalam Mencegah Penyerangan Eksploitasi Web Browser = Analysis of Web Browser Attack and Exploitation Methods Using the Browser Exploitation Framework (BeEF) and Steps to Prevent Web Browser Exploitation Attacks

Lazaruslie Karsono, author

Abstrak

Social Engineering atau dalam Bahasa yaitu rekayasa sosial, merupakan suatu teknik dalam memanipulasi kesalahan yang dilakukan oleh manusia baik disengaja maupun tidak disengaja. Teknik manipulasi ini bertujuan untuk mendapatkan informasi yang bersifat pribadi, penting dan berharga, serta untuk mendapatkan kunci untuk akses masuk terhadap suatu sistem. Dalam dunia kejahatan siber, rekayasa sosial yang memicu terhadap kejahatan peretasan manusia (human hacking) memiliki maksud untuk mengekspos data yang didapat, menyebarkan malware, serta memberikan akses ke dalam suatu sistem yang tidak sah. Serangan rekayasa sosial dapat dilakukan atau terjadi secara online, secara langsung, serta secara interaksi-interaksi lainnya. Salah satu cara untuk melakukan serangan rekayasa sosial, yaitu dengan menggunakan teknik penyerangan phishing (pengelabuan). Dengan melakukan penyamaran seperti orang yang berpura-pura kenal terhadap korban, lalu menggunakan pesan yang dikirim melalui berbagai platform seperti platform sosial media, email, dan bahkan SMS. Ketika pada saat korban melakukan suatu hal pada pesan tersebut seperti mengeklik tautan yang terdapat pada pesan tersebut, maka korban telah berhasil mengekspos data yang dimilikinya kepada penyerang. Dalam skripsi ini, penulis akan membahas mengenai Analisis Metode Penyerangan dan Eksploitasi Web browser dengan Menggunakan Browser Exploitation Framework (BeEF) serta Langkah-langkah dalam Mencegah Penyerangan Eksploitasi Situs Web.
..... Social Engineering or in Bahasa, namely rekayasa sosial, is a technique in manipulating mistake made by humans, both intentional and unintentional. This manipulation technique aims to obtain personal, important, and valuable information, as well as to obtain keys for access to a system. In the world of cybercrime, social engineering that triggers the crime of human hacking has the intent to expose obtained data, spread malware, and provide access to an unauthorized system. Social engineering attacks can be carried out occur online, in person, as well as in other interactions. One way to carry out social engineering attacks is by using phishing attack techniques (deception). By impersonating someone who pretends to know the victim, then using messages sent via various platforms such as social media platforms email and even SMS. When the victim does something to the message, such as clicking on a link in the message, the victim has successfully exposed the data they has to the attacker. In this thesis, the author will discuss the Analysis of Attack Methods and Web Browser Exploitation Using the Browser Exploitation Framework (BeEF) and Steps in Preventing Website Exploitation Attacks.