BROWSER HIJACKING

Definisi

Hijacking adalah kegiatan yang berusaha untuk memasuki (menyusup) ke dalam sistem melalui sistem operasional lainnya yang dijalankan oleh seseorang (hacker). Sistem ini dapat berupa server, jaringan/networking [LAN/WAN], situs web, software atau bahkan kombinasi dari beberapa sistem tersebut. Namun perbedaanya adalah Hijacker menggunakan bantuan software atau server robot untuk melakukan aksinya, tujuanya adalah untuk mengambil data dan informasi pendukung lain, tidak jarang sistem yang dituju juga diambil alih, atau bahkan dirusak.

Browser Hijacking merupakan sebuah kegiatan yang bertujuan untuk menyusup ke dalam browser untuk melakukan session hijacking, yaitu aksi pengambilan kendali session milik user lain setelah sebelumnya "pembajak" berhasil memperoleh autentifikasi ID session yang biasanya tersimpan dalam cookies. Tindakan ini akan melibatkan browser hijacker, yaitu sejenis spyware yang dapat mengendalikan dan mengubah pengaturan pada browser untuk tujuan tertentu.

Kegiatan yang akan dilakukan

- Penjelasan definisi browser hijacking dan browser hijacker
- Identifikasi metode dan alat dalam melakukan browser hijacking
- Identifikasi jenis-jenis browser hijacker dan dampak dari browser hijacking

Referensi

- Barwinski, M.A. (2005).TAXONOMY OF SPYWARE AND EMPIRICAL STUDY OF NETWORK. Thesis from NAVAL POSTGRADUATE SCHOOL.
- Willem Burgers1 , Roel Verdult1 , and Marko van Eekelen1. Prevent Session Hijacking by Binding the Session to the Cryptographic Network Credentials
- Mohammad Mannan. (2009). AUTHENTICATION AND SECURING PERSONAL INFORMATION IN AN UNTRUSTED INTERNET. Thesis from CARLETON UNIVERSITY.
- https://www.terena.org/activities/tf-csirt/meeting27/barroso-hijacking.pdf. Common Browser Hijacking Methods