Perancangan Sistem Identifikasi Serangan Internet Berbasis TPOT Honeypot dengan Klasifikasi Random Forest dan Decision Tree = Design of TPOT Honeypot-Based Internet Attack Identification System with Random Forest and Decision Tree Classification

Ahmad Fakhri Mirfananda, author

Abstrak

Internet telah menjadi salah satu teknologi yang tidak bisa dipisahkan lagi dari kehidupan masyarakat modern. Penggunaan internet telah masuk ke seluruh lapisan masyarakat. Karena sifatnya yang serbaguna, internet telah menjadi salah satu infrastruktur paling esensial di dunia. Banyaknya pengguna akan menimbulkan pihak yang tidak bertanggung jawab. Mereka merupakan individu yang menyalahgunakan internet sebagai media untuk melakukan serangan siber demi mengeksploitasi pihak lain. Penyerang akan menggunakan berbagai metode untuk melakukan eksploitasi. Salah satu metode yang paling sering digunakan oleh penyerang adalah dengan mengirimkan serangan siber. Oleh karena itu, kita harus melindungi sistem kita dari serangan siber. Langkah pertama dapat kita lakukan adalah mengidentifikasi serangantersebut berdasarkan karakteristiknya. Namun untuk membedakannya dari traffic normal, dibutuhkan data yang bisa kita dapatkan dari konsep honeypot yang memancing penyerang untuk melakukan serangan dan mengirimkan data serangan. Untuk melakukan identifikasi secara satu per satu merupakan hal yang sulit dilakukan secara manual.dapat. Namun, hal ini dapat dimudahkan dengan menggunakan artificial intelligence untuk identifikasi pada skala besar. Oleh karena itu, penelitian ini dilakukan untuk membahas penggunaan artificial intelligence yaitu algoritma random forest untuk identifikasi serangan siber yang dikumpulkan melalui honeypot. Hasil penelitian menunjukkan bahwa algoritma random forest dapat memberikan hasil prediksi tipe serangan terbaik dengan parameter jumlah pohon 100 dan tanpa batas kedalaman sebesar 99,48% pada data yang dikumpulkan dengan TPOT.

.....

The Internet has become an inseparable technology from modern society. The use of the internet has reached all layers of society. Due to its versatile nature, the internet has become one of the most essential infrastructures in the world. The large number of users also gives rise to irresponsible individuals who misuse the internet as a medium for cyber attacks to exploit others. Attackers employ various methods to carry out their exploitations. One of the most used methods by attackers is launching cyber attacks. Therefore, we need to protect our systems from these cyber attacks. The first step we can take is to identify the attacks based on their characteristics. However, distinguishing them from normal traffic requires data that we can obtain from a honeypot, which lures attackers to launch attacks and collects attack data. Performing manual identification one by one is a difficult task. However, this can be facilitated by using artificial intelligence for large-scale identification. Hence, this research is conducted to discuss the use of artificial intelligence, specifically the random forest algorithm, for identifying cyber attacks collected through a honeypot. The research results show that the random forest algorithm can provide the best prediction results for attack types with a parameter of 100 trees and no depth limit, achieving an accuracy of 99.48% on the data collected using TPOT.