Analisis karakteristik portable executable files dengan metode static analysis untuk identifikasi penyisipan malware berbasis remnux = Analysis of portable executable files characteristics with static analysis method for malware insertion identification based on remnux

Nindya Viani, author

Abstrak

ABSTRAK
Malware merupakan salah satu ancaman yang sangat berbahaya dalam dunia digital di masa kini maupun di masa yang akan datang. Kini, perkembangan teknologi tidak hanya memberikan keuntungan namun juga menuai tantangan serius. Salah satu tantangan tersebut mengancam sistem keamanan jaringan komputer. Tidak banyak orang yang paham bahwa malware dapat disisipkan dimana saja, khususnya pada berbagai jenis file yang dapat diunduh dari internet. Kondisi ini menunjukkan dibutuhkannya banyak ahli yang mampu menganalisis malware karena perkembangannya semakin kompleks. Oleh karena itu, penelitian ini membahas tentang bagaimana menguji dan menganalisis sebuah executable file dengan memanfaatkan berbagai tools pada sistem operasi REMnux. Hal ini bertujuan untuk dapat mengenali apakah sebuah file tersebut aman atau mengandung malware. Hasil dari penelitian ini menunjukkan bahwa REMnux dapat menjadi sarana yang baik untuk memeriksa ciri-ciri suatu file apakah berupa malware ataukah bukan berdasarkan pengujian terhadap anomali data, metadata integritas file, section entropy, dan function yang dieksekusi oleh executable file tersebut. Selain itu, hasil pengujian juga dapat memperkirakan dampak kinerja malware tersebut apabila eksekusi file tidak sengaja dilakukan dengan cara melakukan reverse engineering, walaupun ada beberapa yang tidak dapat dikonfirmasi secara pasti karena adanya teknik anti-reverse engineering pada file.
<hr>
ABSTRACT<>br>
Malware is one of the most dangerous threats in the digital world today and in the future. Today, technological developments not only give benefits but also reap serious challenges. One of them threatens computer network security system. Not so many people understand that malware can be inserted anywhere, especially on various types of files that can be downloaded from the internet. This condition shows that many experts are required to analyze malware because of its complex development. Therefore, this research discussed about how to test and analyze an executable file by utilizing various tools on REMnux operating system. It aims to recognize whether a file is safe or contains malware. The results of this study indicate that REMnux can be an appropriate tool to check a file rsquo s characteristics in the form of malware or not based on anomalies data check, metadata of file integrity, section entropy, and function that will be executed by that executable file. In addition, the results can also estimate the impact of malware performance if the file execution is not intentionally done by reverse engineering, although there are some cannot be confirmed for sure because of anti reverse engineering techniques on that file.