Analisis Implementasi Host Intrusion Detection System berbasis Teknik String Matching menggunakan tools Yara dalam mendeteksi serangan Malware pada OS Windows dan Linux = Implementation analysis of Host Intrusion Detection System based on String Matching Method using Yara to detect Malware attack on Windows and Linux OS

Aurellio Fishandy, author

Abstrak

Malware merupakan sebuah software berbahaya yang menjadi fokus penelitian bagi para ahli keamanan jaringan dikarenakan kemampuannya yang dapat merusak suatu jaringan maupun perangkat secara efektif dan efisien. Seiring waktu, malware juga turut berkembang mengikuti perkembangan teknologi informasi dan hal ini membuat malware semakin susah untuk di deteksi. Oleh karena itu, para peneliti berbondong-bondong untuk dapat membuat alat pendeteksi malware yang efektif serta efisien menggunakan berbagai macam pendekatan. Alasan tersebut menjadi titik awal yara terbentuk. Sebagai alat pendeteksi atau yang biasa disebut sebagai sistem deteksi intrusi, yara menjadi perangkat lunak yang sering digunakan oleh pengguna jaringan dikarenakan sangat mudah untuk diimplementasi serta menggunakan metode pendekatan yang simpel. Pada penelitian ini, akan membuktikan yara sebagai alat pendeteksi malware yang efektif serta efisien. Selain itu, penelitian ini akan berfokus mengenai strings yang menjadi salah satu faktor penting pada setiap malware serta bagaimana pengaruh strings malware tersebut terhadap yara. Penelitian ini terfokus pada 4 buah malware berbeda yang yakni Backdoor, Spyware, Trojan dan Worm dengan masing-masing 20 buah malware yang akan digunakan sebagai penelitian serta pengujian strings yang nantinya akan dibuat menjadi beberapa rules. Keempat malware tersebut memiliki hasil rata-rata persentase pendeteksian sebesar 81% saat menggunakan rules yang telah disiapkan. Selain itu terdapat beberapa rules yang memiliki persentase diatas 90% saat melakukan pendeteksian terhadap malware.

.....

Malware is a harmful software that have been research focus by network security experts because of their ability to damage a network or devices effectively and efficiently. Over time, malware evolves to become more dangerous following and keeping up with information technology, this makes malware even more difficult to detect by some detection devices. Because of that, many expert trying to make a software that can detect any malware without a problem. That is the beginning of the emergence of yara. As a detection tool or usually known as Intrusion Detection System, Yara becomes a software that frequently used by some user to protect and detect their devices because of its simplicity and convenience. In this research, we will prove that Yara is an effective and efficient malware detection tools. Other than that, we will more focus on how is content of malware can effect on yara. In this research we will focus on 4 different type of malware such as Backdoor, Spyware, Trojan and Worm with 20 pieces of malware that each of the malware will be used as research and testing the strings and later ill be made into several rules in yara. The four malware has an average detection percentage of 81% when using the prepared rules. In addition, there are several rules that have a success percentage above 90% when detecting malware.