ABSTRACT

MALWARE ANALYSIS IN NETWORK TRAFFIC USING WIRESHARK

By

Waskito

1202154223

Malware is a software that is executed or executed automatically that is designed to carry out information theft, control the system, manipulate data, gain access to the host and can be controlled remotely. The spread of malware varies, can be through hardware and through the network so that the spread is very rapid. Malware attacks on computer networks are very large, because the attacker only needs to play behind the scenes. The use of packet capture is done to find out which packets are running on the network in order to see incoming and outgoing data packages. Therefore it is necessary to analyze packet capture to find out malware attacks against suspicious activity on the network and find out the anomaly caused by the malware. To do packet capture analysis using tools such as packet capture analyzers so that data capture packages can be read. The results obtained from detection using a packet capture analyzer are malware behavior and activity when on a network such as the port used and services targeted by malware. From the results of this study, the criteria for attacks carried out by malware will be obtained, categorization based on the impact and risk generated by malware that refers to the access control system, on the network and host network on the network. So that it can be controlled against the output generated based on data obtained from the analysis of data packets on the network.

Keywords: malware, malware analysis, cybercrime, traffic analysis, packet capture, network analyzer