ABSTRACT

MALWARE ANALYSIS IN NETWORK TRAFFIC USING NETWORKMINER

By

JAYSYURAHMAN

1202154199

Malware is a program that has malicious code that is a threat to every user. Malware is created for the purpose of collecting personal information or making damage to network traffic. The spread of malware generally occurs through file attachments that unwittingly users have downloaded files containing malware when using email or website services. Malware is not always on the end-host, it can also be on network traffic, which causes an impact on the network. Therefore, detecting and analyzing malware on network traffic is important because before arriving at end-host malware it will initially be through network traffic. To detect malware on network traffic, PCAP files that contain capture results from monitoring network traffic are needed where the files are analyzed using packet analyzer software, NetworkMiner, to check whether there is malware on network traffic. The results obtained from detection and analysis are malware behavior or activity when on a network such as the port used to attack, and what services are targeted by malware. Based on the analysis, the results obtained are categories of malware based on the impact produced and referring to the access control system aspects, both on network traffic and the hosts on the network. Furthermore, from the malware category it can be made controlling the impact that is produced.

Keyword: ***Malware, Malware analysis, Network anomaly, traffic analysis, Packet capture, Packet Analyzer*.**