Universiti Teknologi MARA

Reducing Honeypot Log Storage Capacity Using Cron Job with Perl-Script

Nur Muhammad Irfan Abu Hassan

Thesis submitted in fulfilment of the requirements for Bachelor of Computer Science (Hons.) Data Communication and Networking Faculty of Computer and Mathematical Sciences

DECEMBER 2018

STUDENT DECLARATION

I certify that this thesis and the project to which it refers is the product of my own work and that any idea or quotation from the work of other people, published or otherwise are fully acknowledged in accordance with the standard referring practices of the discipline.

…….

NUR MUHAMMAD IRFAN BIN ABU HASSAN

2016329461

NOVEMBER 30, 2018

ABSTRACT

Honeypot is a decoy computer system that is used to attract and monitor hackers' activities in the network. The aim of the honeypot is to collect information from the hackers in order to create more secure system. However, the log file generated by honeypot can grow very large when heavy traffic occurred in the system such as Distributed Denial of Services' (DDoS) attack which possess difficulty when it is being processed and analysed by network administrator as it required a lot of time and resources. To address this issue, the objective of this project is to configure a cron job that will run a perl-script which parses the collected data into database in periodically to decrease the log size. Three DDoS attack scenarios were conducted in this project to show the increasing of the log size by sending a different amount of packet per second for 8 hours in each scenario. In scenario 3, the size of the log file has increased to 844MB which causes the honeypot to stop logging information due to the disk space used in the system has reached 100%, and it takes 5 hour 20 minutes to parse the content of the log file into the database which consumed a lot of system resources. At this point, the system performance started to drop off in terms of availability, response time, and processing speed. After using the cron job, the result shown that the log file has been reduced to 118MB, the disk space used has decrease to 91%, and it only takes 40 minutes to parse the log file into the database, thus improved overall system performance. This project had successfully reduced the log size by configuring the cron job to transfer the content of the log file into the database hourly.

TABLE OF CONTENTS