The Performance Analysis Of Malware Attack

Nur Khairani Kamarudin[1*], Nur Nazifabinti Md Hasani[2], Rafiza Ruslan[3], RashidahRamle[4], Nurul Hidayah Ahmad Zukri[5], Iman Hazwam Abd Halim[6]
[1,2,3,4,5,6]*Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Perlis Branch, Malaysia*

*Corresponding author: * nurkhairani@perlis.uitm.edu.my*

Received Date: 1 August 2018
Accepted Date: 12 November 2018

ABSTRACT

People in this new era of modernization nowadays take Internet as one of the vital thing for daily activities. Internet is not only for adults, it is also a needs for people of all ages. However, network vulnerabilities exist in all network that are connected to the Internet. The network mostly are exposed to the malicious software or mostly known as malware. In fact, this malware is growing rapidly and giving a bad impact to the human intervention. The number of attack are increasing rapidly and it comes in various way just to exploit the victims. There are various type of malware attack. For instance, viruses, worms, spyware, rootkits, Trojan horse and botnet are considered as noteworthy threat for the computer network. Some people giving full confidence on the security of data transmission to the network. However, other can access the personal information without them realizing it. The objective of this paper is to detect malware attack using honeypot Dionaea. Malicious file launched was detected by the honeypot and the file was analyzed by using the sandbox tool, Virus Total. This paper found that honeypot Dionaea is helpful in detecting various types of malware attack.

Keywords: *honeypot, malware, Kali Linux, Dionaea, malicious file, memory usage*

INTRODUCTION

Recently, technology keeps expanding rapidly in order to improve human's life. However, without our conscience, network security has become vital to everyone especially to the computer users. The existence of Internet has lead the security as a serious matter. Network security is the method of ensuring the security of data transmission in the network. For instance, cryptography, encryption-decryption, firewall, intrusion detection system and also, honeypots (Paliwal, 2017).

A honeypot is an electronic bait that will trap the person who tends to penetrate the other's computer illegally. The honeypot will appear in the network but in fact, it is a trap to the entire intruders. The honeypot is defined as "information resources whose values the unauthorized use of that resource"(Rase & Deshmukh, 2015). Most honeypots are set up with a firewall. Most honeypots are installed in the network firewall to monitor and track the intruders' activity and what they want from the server. A honeypot is a unique tool to detect and learn about the tactic of the intruders.

The honeypot is a computer system that will act as a fake server to attract the attacker and study the activity of the attacker to gain data in the fake server. The honeypot will simulate the behavior of the real server in the network but in reality, it is isolated and monitored closely. This will able to distract the attacker from attacking the real server.

As an example, people worldwide are using technologies in daily life. This technology contributes many benefits to people mostly. However, all these technologies are exposed to the attack from malware. Malware has been the most common threat to technologies nowadays. Malware attacks their victims through many ways, physically and logically. The malware can be distributed through a website. Not only that, malware can also attack through the website online. This malware attacks a variety of victims for different reasons including to steal sensitive data, disrupt computer operation or acquire access to personal computer system (Mostfa Kamal, Abd Ali, Alani, & Abdulmajed, 2016).

Hence, one of the network security methods which is honeypot is installed and the traffic is then analyzed. There are many types of honeypot that can be used. Dionaea is one of the types of honeypot that can be used. Dionaea can be used to detect malware attack which is now a common problem faced by people all over the world. This honeypot is widely used by network monitoring agent worldwide to detect malware in the network.

RELATED WORKS

Malware Attack

According to the research paper by Fereidooni & Sperduti (2016), the technique used in detecting malware is static analysis of application known as Anastasia. Referring to this paper, static analysis is advantageous especially on an Android device. This is due to the fact that the malware is not being executed but only being analysed. This paper had presented an Android malware detection by using convenient feature to stay away from the application containing malware. Besides, an extensive static analysis on huge amount of data set of 29.864 Android apps was performed. The performance of the analysis was shown in this research paper and it has been proven to be very operative and proficient against malware attack according to the result obtained.

However, Alam & Horspool (2013) had proposed a malware analysis by using Malware Analysis Intermediate Language (MAIL). The process of this analysis at first, the data of binary program must be disassembled and interpreted to a MAIL program. MAIL program can also be used to mark the malware pattern and a control flow graph model (CFG) was built from the interpreted MAIL. A malicious program can be detected once the interpreted CFG matches the database of known malware samples. This method is really useful in detecting the malware. However, this method is only practical at certain situation as it is only able to detect a known malware as it cannot detect the unknown malware.

In the paper by Botacin (2018), malware detection was done through transparent malware analysis. Nowadays, there are two types of transparent analysis which are hardware virtual machine (HVM) and system management mode (SMM). According to this author, HVM technique is only compatible to modern processor such as Intel VT and AMD SVM. This technique permits the code running in the processor. However, in SMM mode, it includes of an executable piece of code located in the BIOS system. This code will be triggered by an interrupt known as system management interrupt (SMI). There is one major drawback of using these two techniques which is both is complex to be developed.

Detection of Threat using Honeypot

In a research paper by (Saud & Islam, 2015), the authors presented the benefit of using honeypot as a security measure to defend the network. According to this paper, one of the purposes of using honeypot includes that it can reverse the attackers' benefit and every single error made by the attackers can alert the system analyst. The other reason is the amount of false-positives is very near to the ground. Instead of the

false-positives reason, the honeypot can slow down the attack and offer a longer time for the authorities to run any other security measure against the attack.
According to Fronimos et. al (2014), the authors argued that old-style network security is insufficient to overcome threat and analysed by a variety of low interaction honeypots such as Dionaea and Honeyd. The analysis from those honeypots displayed how threat can be detected when the honeypot is implemented in a focused network. Eric Hutchins in a paper published by Lockheed Martin Corporation briefly discussed how numerous honeypot can support in messing up any layer of the attack. This whole disruption will cause frustration to the attacker and degrade their confidence to attack the network.

SOFTWARE AND HARDWARE REQUIREMENTS

In this project, there were only one laptop and one wireless modem used. In the laptop, the virtual box was installed and operating system were installed inside it, Kali Linux. Kali Linux was the platform for the configuration of honeypot, Dionaea honeypot and launching the malware attack.

The software used was Kali Linux operating system used to install the Dionaea honeypot. the operating system was installed in the Oracle Virtual Box in the laptop. Msfvenom was the tools to inject the malware into a file and put it into the system before it was detected by the Dionaea honeypot. Next software used was Virus Total tools to analyse the malware in the malicious file.

FINDINGS AND DISCUSSION

Memory Usage before Malware Attack

The memory usage of the system before and after was observed. The memory usage of the system was shown in Figure 1.

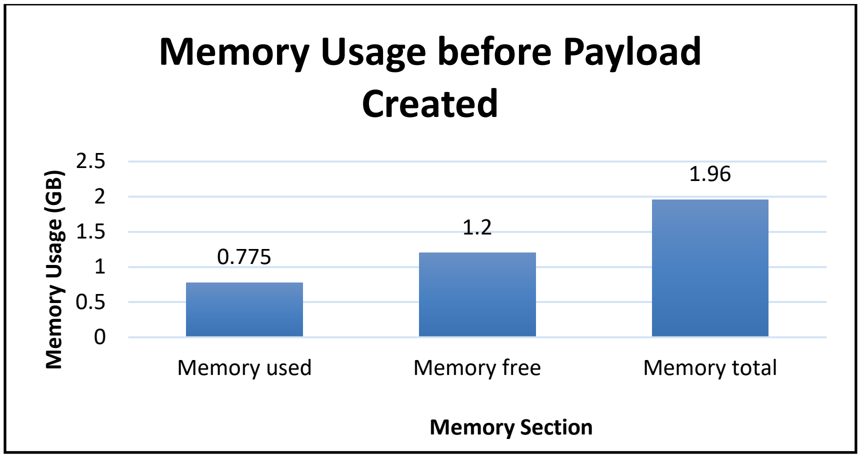

Figure 1: Memory usage before malware attack

Figure 1 shown above, the memory used in the Kali Linux system was 0.775 GB. Meanwhile the memory that were available and free was 1.20 GB. 1.20 GB is quite a huge amount of memory that are available in the system compared to the memory used in the system.The memory total of this operating system was 1.96 GB. Since the malware attack has not been launched yet, the system was not interrupted by the amount of payload in the system. Hence, 38.7 % of the memory has been used before the malware attack has been launched.

Memory Usage after Malware Attack

Next, the malicious file was created and inserted to the system. Afterward, the memory usage of the system was again to be observed. Figure 2 below shows the memory usage after malware attack.

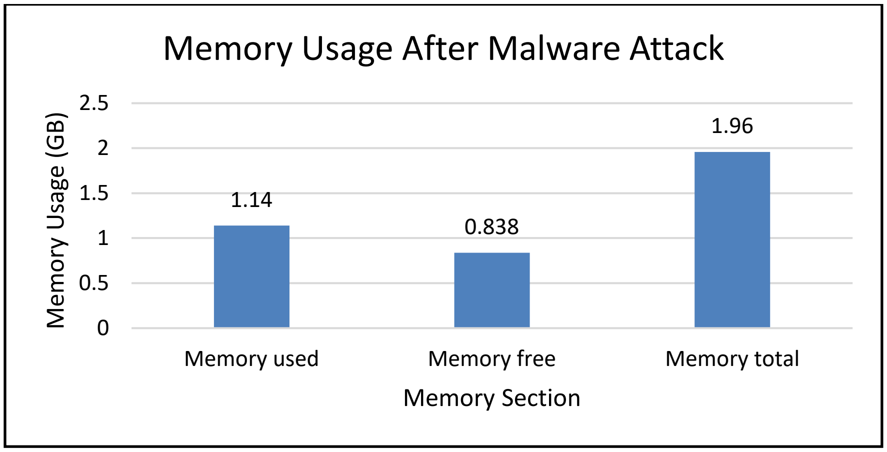

Figure 2: Memory usage after malware attack

Figure 2 above shows that the memory used after the malicious file was created was 1.14 GB. Meanwhile, the available memory in the system was 0.838 GB. The amount of the available memory was low. The memory total was remain the same, 1.96 GB. Hence, the memory used after the attack was 41.8%.

Result Analysis

The memory used before the malicious file run in the system was fewer than the memory after the payload has been created. The memory used before the malware attack was 0.775 GB and was increased to 1.14 GB after the payload was executed in the Kali Linux system.Meanwhile the memory available before the malware attack was greater than after attack which was 1.2 GB, before attack and 0.838 GB, after the attack. The graph shows the total memory for the system before and after the malware attack was remain the same which was 1.96 GB.

CONCLUSION AND RECOMMENDATION

The objectives of the project are to set up a Dionaea honeypot in Kali Linux and to detect and analyze the malicious file detected by Dionaea honeypot by using sandbox tool. This research project was implemented by using a laptop and one wireless modem. The laptop contained the VirtualBox which the Kali Linux operating system is installed. Kali Linux is act as the platform for the Dionaea Honeypot to be configured. After the honeypot was activated, the memory usage of the system was observed. On the other hand, the malicious file was created and run in the other terminal in the Kali Linux by using the msfvenom tool. Once the file has been made, the honeypot was successfully detected the malicious file and the file was analyzed in the Virus Total website. After the malware was analyzed, the memory usage of the operating system was captured and observed.

REFERENCES

Frei, S., & Zürich, E. T. H. (2007). SQL Slammer Worm Network Security - Live Demonstration Worm Features Security Bulletin Spread of worm Protection ƒ References. *Swiss Federal Institute of Technology Zurich*.

Highleyman, W. H. (2016). US Internet Traffic Comes to a Halt. *The Availablity Digest*, (October 2006), 2006–2011. Retrieved from www.availabilitydigest.com

Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S., & Weaver, N. (2003). Inside The Slammer Worm. *IEEE Security and Privacy*, *1*(4), 33–39. https://doi.org/10.1109/MSECP.2003.1219056

Mostfa Kamal, S. U., Abd Ali, R. J., Alani, H. K., & Abdulmajed, E. S. (2016). Survey And Brief History On Malware In Network Security Case Study : Viruses , Worms And Bots. *ARPN Journal of Engineering and Applied Sciences*, *11*(January).

Paliwal, S. (2017). Honeypot: A Trap for Attackers. *International Journal of Advanced Research in Computer and Communication Engineering*, *6*(3), 842–845. https://doi.org/10.17148/IJARCCE.2017.63197

Rase, S. B., & Deshmukh, P. (2015). Summarization of Honeypot- A Evolutionary Technology for Securing Data over Network , And Comparison with some Security Techniques. *International Journal of Science and Research*, *4*(3), 1440–1445.

Sharp, R. (2009). An Introduction to Malware Classification of Malware. *Cert-UK*, 1–28. https://doi.org/10.1017/CBO9780511623806

Snyder, C. (2017). Too Connected To Fail And What We Can Do About It. *Belfer Center for Science and International Affairs Harvard Kennedy School*, 54. Retrieved from https://www.belfercenter.org/publication/too-connected-fail