Universiti Teknologi MARA

IDSpoof: Intrusion Detection to Detect Malware

Muhammad Khairie Bin Ismail

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

July 2020

ACKNOWLEDGMENT

Alhamdulillah praises and thanks to Allah because of His Almighty and His utmost blessings, I was able to finish this research within the time duration given. Primarily, my special thanks go to my supervisor, Kamarul Ariffin Abdul Basit that conducted and helped me prepared this proposal successfully.

Special appreciation also goes to my beloved parents, which helps a lot in terms of finances and passion.

Finally, I would like to give my gratitude to all of my dearest friends for giving support to me as I have a problem to identify the related project of my project.

ABSTRACT

Nowadays, people all over the world like to store their data over the Internet because it is easy for them to retrieve and store it. Unfortunately, they are exposed to the cyber-crime like data theft because of the lack of security in their device. People usually did not have a security tool for their network. To prevent data theft, we need to monitor and identify the packet, which is appropriate in the network. It is important to prevent the malicious packet from going through the network because it may affect the privacy's data of the user. IDSpoof was developed to monitor the network packet and expected to have the functionality of the system. The methodology was used to develop the project using research framework. After this project is developed, the IDSpoof is expected to be used by the user and the result demonstrate successful decrement of data theft among the user. Then, user network will be more secured and protectable.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Background of study

An Intrusion Detection System is an application which is used to control the network and protect it against the intruder. New application areas for computer network have emerged with the rapid growth of Internet-based technology (PeymanKabiri and Ali A. Ghorbani, 2005) The LAN and WAN technologies have advanced in areas such as business, finance, manufacturing, security and healthcare sectors. All these areas of operation rendered the network an enticing target for exploitation and a great weakness for the government. The organization's internal systems are used by unauthorized users or hackers to gather information and trigger vulnerabilities such as Computer bugs, Lapse in operation, leaving systems to default config (Christopher Low, 2005). Figure 1.1 show Intrusion Detection System.

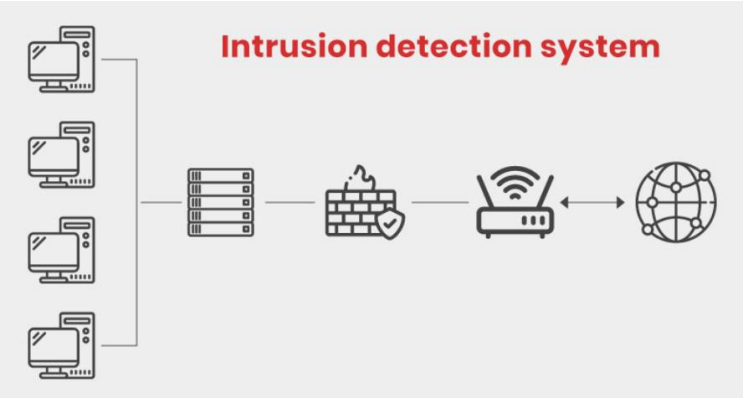

Figure 1.1: Intrusion Detection System

Retrieved from https://blog.eccouncil.org/how-do-intrusion-detection-systems-ids-work/