Universiti Teknologi MARA

Botnet Detection using Automated Script

NORFATHIN BINTI ROSLI

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

February 2020

ACKNOWLEDGEMENT

Firstly, Alhamdulillah thank Allah for giving me the opportunity to embark on my degree and for completing this long and challenging journey successfully.

Alhamdulillah. First of all, I would like to express my highest gratitude to my supervisor, Sir Muhd Azizi Muhamad Ariffin for his guidance, advice and support in order to complete this final year project proposal. I really appreciate it.

Thanks to all the lecturers in the course of Bachelor of Computer Science (Hons) Data Communication & Networking at UITM Shah Alam for their patience and kind advice during the process of completing this proposal.

Lastly, thank you to all those who supporting me in any way during the completions of this proposal report by discussing, sharing or exchanging ideas and everyone who are directly or indirectly involved in writing this report.

Thank you so much.

ABSTRACT

This paper is about a Botnet Detection using Automated Script, the programming language is and the operating system is Windows 7. The project is dedicated for Network and Security Analyst to develop better algorithm for botnet detect and prevents. This Botnet are malicious software that controlled networks of hijacked computers and aiming for distributed coordinate network initiate various malicious over network activities including click fraud, spam, and phishing. Nowadays, as we know the virus or malware spread can be so fast and usually hard to detect. This simulation is to detect the Botnet presence and identifying its behaviour. This project using Python script to kill the process of Botnet.

TABLE OF CONTENT

CHAPTER 1

INTRODUCTION

This chapter provides an overview of the research project and discussion about the project background, problem statements, project objectives, scope, the significance of project, and limitation of project.

1.1Background of Study

Botnets or also known as is ‘robot network’ controlled by central command server. This botnet are malicious software that controlled networks of hijacked computers and aiming for distributed coordinated network initiate various malicious over network activities including click fraud, spam, and phishing.

Malicious software or malware is any program or file that intentionally damage computer, or infiltrate, server or computer network, it also defined as malicious code. Malware is specially to be hidden so they can remain inside a system for a certain period of time without knowledge of the system owner or user.

The virtualisation technique provides the complete simulates the underlying hardware to allow an unmodified operating system to be run in isolation. In this project, virtual machine is a software solution that implements virtualisation and Windows 7 as operating system to be install in virtual machine.

1.2Problem Statement

An increasing number of articles in the media report an increasing crime involving botnets (Thomas, 2015). Botnet can contain thousands of hosts and can be used to perform a variety of cyber attacks, especially by flooding target networks and devices with too much traffic and stealing data from infected hosts.