UNIVERSITI TEKNOLOGI MARA

DETECTION AND PREVENTION OF IOT-BASED DDOS ATTACK ON IPV6

MOHAMMAD IHTISYAMUDDIN MOHD ZAIDI

BACHELOR OF COMPUTER SCIENCE (Hons.)
NETWORKING AND DATA COMMUNICATION

JULY 2021

ACKNOWLEDGEMENT

First and foremost, thank God for allowing me to embark on my degree and for completing this long and challenging journey successfully.

Special thanks to my supervisor Muhammad Azizi Mohd Ariffin, for helping me with this project and for guidance and support. His willingness to encourage and inspired me much to work harder in finishing this project until the end.

Finally, an honorable mention goes to my families and friends, especially my beloved parents, who have given me all the support from various aspects.

ABSTRACT

The Internet of Things (IoT) has been continually growing in the last couple of years, and with the issues of IPv4 address exhaustion, many IoT devices started to adopt IPv6 protocol. These IoT devices appeared to be vulnerable to many kinds of attacks. Attackers can turn these smart devices into botnet to conduct Distributed Denial of Services (DDoS) attacks. Currently, there is no DDoS prevention mechanism able to address IoT-based DDoS attacks using the IPv6 protocol. To address this threat, this paper proposed a solution using Python mitigation script that can detect DDoS attack by collecting data from system parameters such as CPU, memory, and network utilization. The proposed solution also provides a DDoS attack prevention mechanism using the Ubuntu default firewall configuration tool, Uncomplicated Firewall (UFW). The result from the mitigation test shows that the system is effective against DDoS attack on IPv6. This project seeks to help network administrators and smart homeowners to prepare and reduce the risk of being a victim of IoT-based DDoS attacks.

TABLE OF CONTENTS

CONTENT **PAGE**

CHAPTER 1

INTRODUCTION

1.1 Background of Study

The Internet of Things (IoT) refers to computing devices, machines, or objects that are connected to the Internet and transfer data over a network. According to Gartner (2017), the number of IoT devices connected to the Internet will be around 20.4 billion by 2020. IoT devices lack processing power and memory. Thus, it is often overlooked and advances security measures were not installed (Hallman et al., 2017). There is a high possibility these unsecured IoT devices such as CCTV cameras, smart refrigerators, smartwatches, and webcams are attacked by hackers and turned into a malicious botnet. Botnet refers to a group of computers or IoT devices that have been infected by malware and becomes under the control of the botmaster (Sikkanan & Kasthuri M., 2019). The botmaster can remotely control and instruct them to do various cyber-attacks such as sending spam emails, stealing target information, and performing Distributed denial-of-service (DDoS) attacks.

DDoS is one of the network attacks that is commonly used by attackers. The DDoS attack attempts to overwhelm the targeted server, websites, or network with a flood of internet traffic from many different sources such as hacked computers and botnet until the victim's operation is inoperable. The DDoS attack can happen on both IPv4 and IPv6 addresses. Unfortunately, many organizations are not prepared to mitigate IPv6 based DDoS attacks due to their relatively immature nature as network structures (Zhong & Chen, 2020). It is hard to prevent IoT devices from becoming a botnet. Still, organizations can undoubtedly protect their networks by implementing a real-time and automated solution to detect and eliminate the threats from entering a network.