CHAPTER 1
INTRODUCTION

1.1 Background

The evolution of science and technology is faster now. Information has been digitalized to facilitate human life. Companies are also growing rapidly due to digitalization and the internet for global business. However, the development of this internet era raises new threats. Many kind of attacks exist and threat the security system of this internet era. The development of digital world also makes the security issue become a hot topic [1]. The security issue or cyber-attacks may also appear in workplaces, that can be caused by the employees themselves or external attack. Based on this issue, building a smart security system to protect the used work devices when connected to office network is a required solution to overcome the issue.

Some security systems exist, including Firewall and Intrusion Detection System (IDS). Those two are widely used as the network security systems [2]. Firewall works as the wall that limits the computer network, so it can control all activities in the network. This technology of security system is one of the major factors to evaluate performance [3]. Even, firewall set up is not a fancy thing to protect private networks sites. IDS detects the attacks and alerts them, so the attack can be identified earlier. IDS itself has been implemented in several papers. Haystack by Tracer Applied Science, Inc., a prototype of IDS that was applied in multi-user Air Force computer system. The method used in IDS is analyzing the bad behavior of network [4].

Furthermore, the implementation of IDS is usually related to Snort. Snort is an application to detect the network traffic that can prevent and do real-time traffic analysis in Internet Protocol (IP) network. The collaboration of HIPS and Snort is widely implemented as the cyber security system in companies.

In 1998, Martin Roesch from Stanford Telecommunications, Inc. and is the inventor of Snort published a paper about Snort as the 'Lightweight IDS' because it is a perfect role for it. It is a cross-platform network sniffing tool. Snort can be configured to be left while running in a long period [5]. It does not require monitoring maintenance and for that reason, Snort is considered as the revolutionary of network security infrastructure. Martin Roesch also found the *Sourcefire* company

to manage the development of Snort in 2001. Now, Snort is taken by *Cisco* since 2013 which bought it from *Sourcefire* [1].

IDS continued to grow until it developed a new security system called Intrusion Prevention System (IPS). Compared to IDS, this system not only can detect suspicious behaviors and attacks, but also can prevent by dropping them. This security system is the result of a combination of two cybersecurity systems that has been mentioned above, Firewall (access control) and IDS [6].

This thesis analyzes the capability of IPS against Denial of Service (DoS) attacks in office network. DoS attack can cause an unavailability of server and make the server cannot run its functions properly [7]. The effect is that can harm business of companies. Several cases have occurred, one of them was experienced by one of the biggest Information Technology (IT) companies, Sony Playstation that caused the users cannot access because there was a service failure. This attack has been a major cause that disturbs the user's work devices in workplaces when connected to office network. Intrusion Prevention System (IPS) appeared to be the security system to protect them from DoS attacks. The research about this security system has been done before and definitely has differences. As in previous research on "Implementation and Analysis of Virtual Network Security Against DoS and DDoS Attack with HIPS Snort" by Ivan Saputra Zebua in which the research studied about the ability of HIPS Snort in preventing DoS and DDoS attacks in virtual network [8]. However, that previous research is different because this thesis focuses about the implementation and analysis of network security in real network against DoS attack with HIPS Snort. Furthermore, this thesis tests about the ability of HIPS Snort in preventing the DoS attack in real network.

This thesis uses Raspberry Pi to implement it in real network with HIPS snort to prevent the DoS attack. This thesis builds a Smart Security in A Box by realizing the security system that previously only implemented in virtual network. The combination of IPS and a Snort application is used in this thesis called Host Intrusion Prevention System (HIPS) Snort. The realization is going to be built in a Raspberry Pi as the firewall and the HIPS Snort is installed on it.

Raspberry itself is a single-board, tiny, and affordable computer that is usually used to compile or to learn the programming of Internet of Things (IoT) or robotic projects [9]. In addition to that, Raspberry Pi in this thesis as the host of IPS is required to be configured as a router, so the network that flow through the Raspberry Pi is able to be captured and scanned. This Smart Security in A Box System is expected to be useful to prevent the DoS attacks that flow through the router which in this case the Raspberry Pi.

This thesis is important to be done because it builds the Firewall Security System in router Raspberry Pi that is installed and configured with HIPS Snort and it is also useful to protect the office network against DoS attacks to expedite the workflow of the office. Therefore, the research about Implementation and Analysis of Network Security in Raspberry Pi is feasible to do.

1.2 Problem Formulation

The problem considered in this thesis is the Denial of Service (DoS) attack in the form of SYN Flood and UDP Flood in companies that is usually caused by the employees themselves. This may disturb both the users and the devices performance. In workplaces, SYN Flood and UDP Flood usually attack the work devices of the employees and indirectly harm the performance of the company. Therefore, SYN Flood and UDP Flood may harm companies in running their business. These kind of DoS attacks have been a major problem in cyber world.

1.3 Objectives

The objective of this undergraduate thesis is to build a smart security in a box with Raspberry Pi as the firewall and to study the capability of HIPS that is installed on a Raspberry Pi against the DoS attacks. According to [7], the security system using HIPS network has to be implemented not only in virtual network.

Therefore, this thesis uses Raspberry Pi to implement the security system. The used DoS attacks are SYN Flood and UDP Flood to test the HIPS Snort ability to protect the client or user's work devices (PC or Laptop) against the SYN Flood and UDP Flood.

1.4 Scope of Works

The work boundaries in this undergraduate thesis research are as follows:

1. Raspberry Pi is built to work as a router.
2. Host Intrusion Prevention System Snort is installed on the Raspberry Pi.
3. The targeted packets dropped is determined by the capability of Raspberry Pi.
4. SYN Flood and UDP Flood are the DoS attacks that tests the Smart Security in A Box System.
5. The CPU and Memory usage of Raspberry Pi are observed.

1.5 Research Method

The research method used in this thesis are:

1. Literature Study
   Collect data from journals, papers, articles, books, and other thesis related to Host Intrusion Prevention System (HIPS), Snort, Raspberry Pi, Cyber Security, and DoS Attack. Then, discuss the material with the Supervisor.

2. Raspberry Pi as Router Configuration
   Design security system uses Raspberry Pi that is configured to work as router.

3. HIPS Snort installation
   Install an HIPS Snort on Raspberry Pi to complete the Smart Security in A Box System.

4. Simulation test and research validation
   An experimental DoS attack deployment to test the performance of the Smart Security in A Box.

5. Data collection and data analysis
   Collect and analyze the data include the capability of the security system in preventing the malicious data packets.

1.6 Undergraduate Thesis Organization

The rest of this thesis is organized as follows:

- Chapter 2 BASIC CONCEPT
  This chapter contains the basic concept and theory explanation.

- Chapter 3 SYSTEM PLANNING
  This chapter contains the workflow and the system plannig design flow.

- Chapter 4 PERFORMANCE EVALUATION
  This chapter contains the simulation and examination steps, test result, and test analysis.

- Chapter 5 CONCLUSIONS
  This chapter contains the conclusion and suggestion.