CHAPTER I
INTRODUCTION

A. Background of Study

The security and confidentiality problem of computer network is improving now. In the last years, the dangerous traffic like malicious and ddos (distributed denial of service) is improving. There are companies which offer some services to public, getting attack which is caused they cannot offer user demand (KasperskyLab, 2013).

The installation of firewall, antivirus, IDS (Intrusion Detection System) / IPS (Intrusion Prevention System) and other security applications are available. But they are expensive. For rich companies, there will be not problem to install an expensive security application. But it will be a big problem for poor companies. Open source application can be a solution. Almost open source applications are free, and user can develop the application.

Nowadays, IDS is one of famous security tools which are used. IDS prevent hacker or intruder to attack the company's system. Administrator can collect information about attack from IDS. Administrator also uses it for knowing whether people try to attack the network or specific host.

There are some IDS open source application such as Snort, Bro, Ossec, Prelude, and Suricata. The characteristic of good IDS applications are they have accuracy, performance, completeness, fault tolerance, and scalability. With these characteristics, IDS application can help administrator to minimize some errors in taking action.

Based on the facts above, the writer tries to make analysis and evaluation from three applications. Applications are Snort, Bro, Suricata.

B. Problem Statement

The problem statement of the research is “What are the advantages and disadvantages of Snort, Bro, and Suricata as Intrusion Detection System?”.

C. Limitation of Study

Problem limitation is used to avoid deviation and dilation of subject matter, so research can be more focus. Problem limitations are:

1. The system is only used to monitor network computer activity. Especially if there is an attack to the server.
2. IDM system is built uses Snort, Bro, and Suricata as IDS application in computer network with Linux Ubuntu Server 12.04 Operating System.
3. The traffic data which is seen in the research is limited by data package. Especially data package which is connected to the server security.
4. The characteristic of good IDS applications are they have accuracy, performance, completeness, fault tolerance, and scalability.

D. Objective

The objective of the research is to know the advantages and disadvantages of Snort, Bro, and Suricata as Intrusion Detection System application.

E. Benefit

The benefits of the research are:

1. For User

   The research can help network administrator to choose IDS application. Especially to identify and resolve network attacks.

2. For Writer

   The writer learn new thing to get other experiences besides learn in college.

3. For Public

   People know the advantages and disadvantages of Snort, Bro, and Suricata in order to know and resolve network attacks.

F. Report Organization

Report organization to make it easier to be understood is as follows:

CHAPTER I INTRODUCTION

Chapter I consist of background of the study, problem statement, problem limitation, objective, benefits, and report organization.

CHAPTER II LITERATURE REVIEW

Chapters II consist of theories that used in the research, design, construction.

CHAPTER III RESEARCH METHOD

Chapters III consist of explanation about what method that the writer uses in the research and implementation.

CHAPTER IV RESULT and ANALYSIS

Chapter IV will explain result and analysis of the application.

CHAPTER V CLOSING

Chapters V consist of conclusion and suggestion based on research.