PROJECT REPORT

PACKET SNIFTER PROGRAM USING PYTHON FOR MALWARES IDENTIFY

Don Fransiskus Chandra Da Silva
13.02.0114

Faculty of Computer Science
Soegijapranata Catholic University
2017
APPROVAL AND RATIFICATION PAGE

PACKET SNIFTER PROGRAM USING PYTHON FOR MALWARES

IDENTIFY

by

DON FRANSISKUS CHANDRA DA SILVA – 13.02.0114

This project report has been approved and ratified

by the Faculty of Computer Science on July, 12, 2017

With approval,

Supervisor,

Suyanto F.A. Ir., M.Sc

Examiners,

1.)
Rosita Herawati, ST., MT
NPP : 058.1.2004.263

2.)
Hironimus Leong, S.Kom., M.Kom
NPP : 058.1.2007.273

3.)
Shinta Estri Wabbyuningrum, S.Si., M.Cs
NPP : 058.1.2007.272
STATEMENT OF ORIGINALITY

I, the undersigned:

Name      : Don Fransiskus Chandra Da Silva
ID        : 13.02.0114

Certify that this project was made by myself and not copy or plagiarize from other people, except that in writing expressed to the other article. If it is proven that this project was plagiarizes or copy the other. I am ready to accept a sanction.

Semarang, July 12, 2017

[Signature]

Don Fransiskus Chandra Da Silva
13.02.0114
ABSTRACT

Today the internet is becoming a basic need in terms of communication, sharing information and transaction over long distances. One of the problems in the internet is malware. Malware is software that can damage or disrupt the computer operating systems. The spread of malware can be through email or any application that uses the internet media. Whenever the computer is connected to the internet, there is possibilities to be attacked by malware.

In order to avoid malware attacks, special knowledge is required about the type of malware and how the spread process occurs. This can be done by monitoring and checking data traffic on computer networks. The tool that can be used is packet sniffer. Packet sniffer is a tool that can collect packet data in the network for the monitor. Packet sniffer is useful for analyzing disturbances, what data is received and transmitted over the network and shows information about interacting computers. In this project, a packet sniffer program will be created. Packet data captured with this program, can be analyzed to determine the traffic data activity that is malware or not. With a known malware attack then the right action can be done immediately.

Packet sniffer program is created with python. For monitoring data which generated by a packet sniffer, web-based program will be created by using PHP programming language. This tool only helps in recording the data traffic in the local network to be analyzed. To get the activity pattern of malware, the results depends on the expertise of the users in analyzing the network.

Keyword: Internet, Malware, Network, Packet Sniffer
PREFACE

This project report have six chapter. The first chapter is an introduction to project that will be used. Chapter 1 contains background, scope, and objective. In this chapter it will be explained why this project is created, what is the objective, and how the output look like.

Chapter 2 contains literature that is used as a study in building this project. It is also explained in this chapter about the difference between the literature study and the project that will be made.

In Chapter 3, every step in creating this project will be discussed. While in Chapter 4, there are analysis and design that will be used to create this project. The analysis part discuss about problem that needed to be solved. The solution then explained in design part, which is also contain use case, flow chart, and DFD.

Chapter 5 discuss about implementation of this project, and then will be explained in testing. Chapter 6 contains conclusion of making this project. This chapter also contains suggestion that can be developed in further research.
# TABLE OF CONTENTS

Cover.........................................................................................................................................................i  
APPROVAL AND RATIFICATION PAGE................................................................................................. ii  
STATEMENT OF ORIGINALITY.............................................................................................................. iii  
ABSTRACT.................................................................................................................................................. iv  
PREFACE.................................................................................................................................................. v  
TABLE OF CONTENTS........................................................................................................................... vi  
ILLUSTRATION INDEX............................................................................................................................ vii  
INDEX OF TABLES................................................................................................................................... viii  
CHAPTER 1 INTRODUCTION................................................................................................................... 1  
1.1Background........................................................................................................................................ 1  
1.2Scope.................................................................................................................................................. 1  
1.3Objective........................................................................................................................................... 2  
CHAPTER 2 LITERATURE STUDY........................................................................................................... 3  
CHAPTER 3 RESEARCH METHODOLOGY............................................................................................ 5  
CHAPTER 4 ANALYSIS AND DESIGN.................................................................................................... 6  
4.1Analysis............................................................................................................................................... 6  
4.2Design.............................................................................................................................................. 12  
CHAPTER 5 IMPLEMENTATION AND TESTING................................................................................ 16  
5.1Implementation............................................................................................................................... 16  
5.2Testing............................................................................................................................................... 16  
CHAPTER 6 CONCLUSION..................................................................................................................... 17  
REFERENCES......................................................................................................................................... 17  
APPENDIX............................................................................................................................................... A  

vi
ILLUSTRATION INDEX

Illustration 4.1: Packet data delivery process in the OSI model.................................6
Illustration 4.2: PDU Encapsulation..............................................................................9
Illustration 4.3: Network topology for running Packet Sniffer program...............13
Illustration 4.4: Packet Sniffer Flowchart................................................................14
Illustration 4.5: Packet Sniffer Database......................................................................15
Illustration 5.1: Run the Packet Sniffer program......................................................20
Illustration 5.2: PC Internet access and PC B did not access anything...............20
Illustration 5.3: Dashboard Page.................................................................................21
Illustration 5.4: Page to show all packets TCP and UDP........................................22
Illustration 5.5: Page to show packets TCP only.....................................................22
Illustration 5.6: Page to show packets UDP only.....................................................23
Illustration 5.7: PC A infected by WannaCry malware and PC B not yet infected. ..............................24
Illustration 5.8: PCB is infected by Malware...................................................................24
Illustration 5.9: Dashboard page after PCA and PCB is infected by malware...........25
Illustration 5.10: TCP page after PCA and PCB is infected by malware...................26
## INDEX OF TABLES

Table 4.1: IPv4 Header Fields ................................................................. 10
Table 4.2: TCP Header Fields ............................................................... 11
Table 4.3: UDP Header Fields ............................................................... 12