



**PROJECT REPORT**

**Intrusion Detection System (IDS) Using Genetic  
Algorithm And Port Scanning**

Budi Santoso

07.02.0055

2011

**COMPUTER SCIENCE FACULTY**

**SOEGIJAPRANATA CATHOLIC UNIVERSITY**

Jl. Pawiyatan Luhur IV / 1, Bendan Duwur, Semarang 50234

Telp (024)-8441555 (Hunting) Web : <http://www.unika.ac.id>

Email : [ikom@unika.ac.id](mailto:ikom@unika.ac.id)

# APPROVAL AND RATIFICATION PAGE

## PROJECT REPORT

### Intrusion Detection System (IDS) Using Genetic Algorithm

### And Port Scanning

This Project Report has been approved and ratified by Dean of Computer Science Faculty on 20<sup>th</sup> January 2011

With the approval,

Examiner,

Examiner,

Robertus Aji Setiawan, ST, McompIT  
NIP: 058.1.2004.264

Suyanto EA, Ir, M.Sc  
NIP: 058.1.1992.116

Examiner,

Examiner,

Gregorius Hendita Artha Kusuma, S.Si, M.Cs  
NIP: 058.1.2008.277

Marlon Leong, S.Kom, M.Kom  
NIP: 058.1.2007.273

Supervisor,

Dean of Faculty of Computer Science,

Rosita Herawati, ST, MIT  
NIP: 058.1.2004.116

Marlon Leong, S.Kom, M.Kom  
NIP: 058.1.2007.273

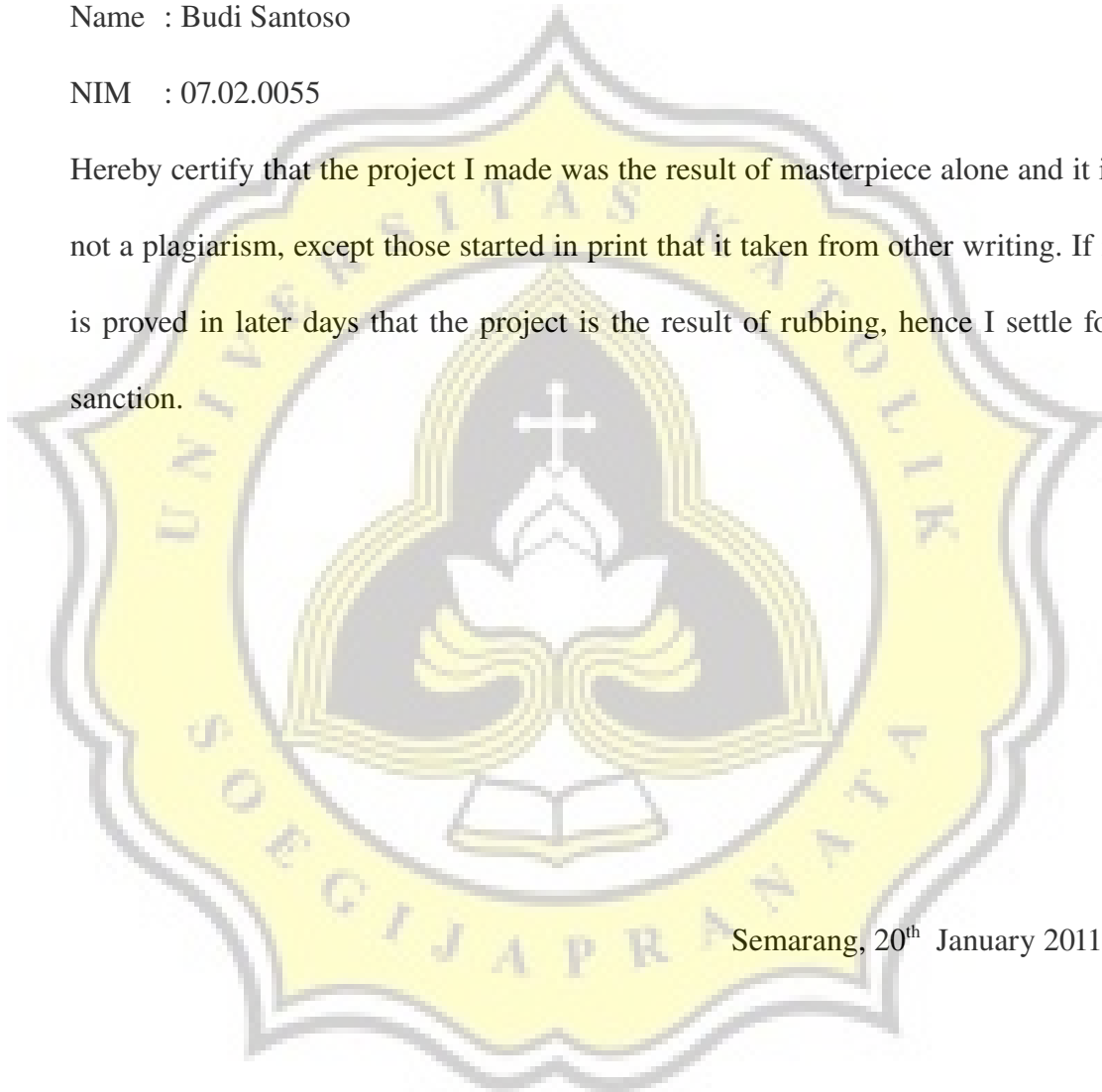
## STATEMENT OF ORIGINALITY

I, the undersigned

Name : Budi Santoso

NIM : 07.02.0055

Hereby certify that the project I made was the result of masterpiece alone and it is not a plagiarism, except those started in print that it taken from other writing. If it is proved in later days that the project is the result of rubbing, hence I settle for sanction.



Semarang, 20<sup>th</sup> January 2011

Budi Santoso  
NIM. 07.02.0055

# FOREWORD

Finally, I could finish my project with the title of: Intrusion Detection System (IDS) Using Genetic Algorithm And Port Scanning. There are a lot of experience when working on this project, whether bad or good. These things made me become a better and closer to god. on this occasion I would like to thank:

1. My Lord, Jesus Christ that give me bless to finish this project
2. My parents, my brother, my sister and my big family for their support.
3. Mrs. Rosita Herawati, ST, MIT as my supervisor for helping, guiding, and giving me ideas and advice.
4. Other lecturers in the faculty of computer science that guided me while studying in this faculty.
5. All my friends who provide support and assistance during the work on this project.
6. Others who provide assistance and support that I can not mention one by one.

Last but not least, I would like to apologize for any mistake I have done in completing this project, and accordingly constructive critics and suggestions would be welcome.

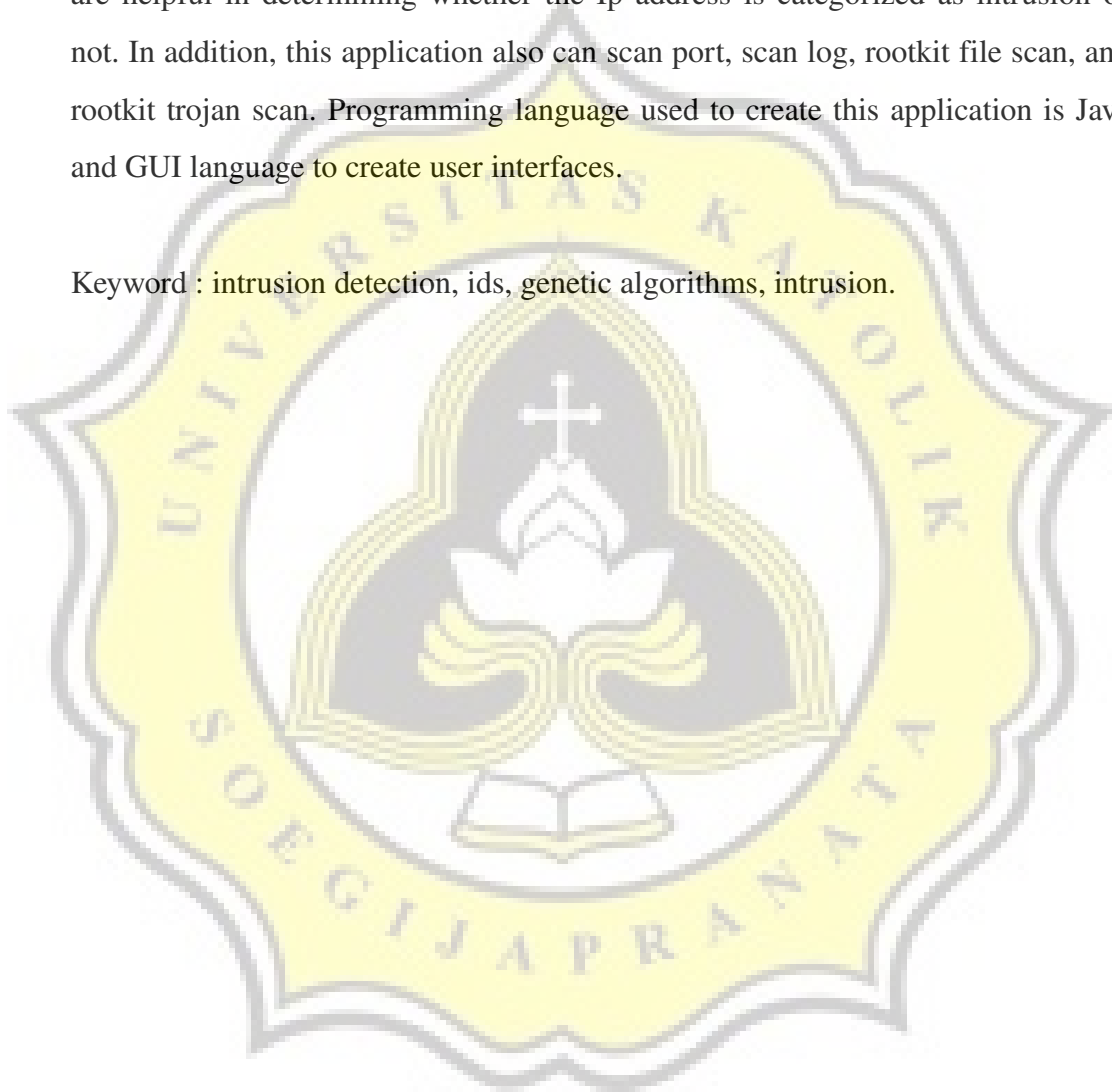
Semarang, 20<sup>th</sup> January 2011

Budi Santoso

## **ABSTRACT**

This application is used to detect intrusion in a computer. To detect intrusion use genetic algorithms adoption. Value of fitness in genetic algorithms are helpful in determining whether the Ip address is categorized as intrusion or not. In addition, this application also can scan port, scan log, rootkit file scan, and rootkit trojan scan. Programming language used to create this application is Java and GUI language to create user interfaces.

Keyword : intrusion detection, ids, genetic algorithms, intrusion.



# Table of Content

|                                      |      |
|--------------------------------------|------|
| APPROVAL AND RATIFICATION PAGE.....  | i    |
| STATEMENT OF ORIGINALITY.....        | ii   |
| FOREWORD.....                        | iii  |
| ABSTRAC.....                         | iv   |
| Table of Content.....                | v    |
| Table of Figure.....                 | viii |
| Table of Tables.....                 | x    |
| CHAPTER I Introduction               |      |
| 1.1. Background.....                 | 1    |
| 1.2. Scope.....                      | 2    |
| 1.3. Objective.....                  | 2    |
| CHAPTER II Literature Study          |      |
| 2.1. Linklist.....                   | 3    |
| 2.2. Tree.....                       | 4    |
| 2.3. Addopted Genetic Algorithm..... | 5    |
| CHAPTER III Planning                 |      |
| 3.1. Research Methodologies.....     | 9    |
| 3.2. Project Management.....         | 10   |
| CHAPTER IV Analysis and Design       |      |
| 4.1. Use Case Diagram.....           | 11   |
| 4.2. Class Diagram.....              | 12   |
| 4.2.1. PortScanner.....              | 13   |
| 4.2.2. NodePath.....                 | 13   |
| 4.2.3. NodeMessage.....              | 14   |
| 4.2.4. FileWrite.....                | 14   |
| 4.2.5. Linklist.....                 | 15   |

|   |    |
|---|----|
| 4.2.6. NodeTree.....                        | 15 |
| 4.2.7. NodeIP.....                          | 16 |
| 4.2.8. SearchString.....                    | 17 |
| 4.2.9. Directory.....                       | 18 |
| 4.2.10. NodeSearchResult.....               | 19 |
| 4.2.11. BinaryTree.....                     | 19 |
| 4.2.12. GA.....                             | 20 |
| 4.2.13. FileRead2.....                      | 20 |
| 4.2.14. Main.....                           | 21 |
| <b>CHAPTER V Implementation and Testing</b> |    |
| 5.1. Implementation                         |    |
| 5.1.1. Search File rootkit.....             | 23 |
| 5.1.2. Scan port.....                       | 25 |
| 5.1.3. scan log.....                        | 26 |
| 5.1.4. scan trojan rootkit.....             | 26 |
| 5.1.5. Scan IP.....                         | 28 |
| 5.2. Testing                                |    |
| 5.2.1. Scan log.....                        | 32 |
| 5.2.2. Scan file trojan.....                | 32 |
| 5.2.3. Scan trojan rootkit.....             | 33 |
| 5.2.4. Scan IP.....                         | 33 |
| 5.2.5. Scan all port.....                   | 34 |
| 5.2.6. Scan single port.....                | 34 |
| 5.2.7. Write iptables (firewall).....       | 35 |
| 5.2.8. iptables before insert rule.....     | 35 |
| 5.2.9. iptables after insert rule.....      | 36 |
| <b>CHAPTER VI Conclusion</b>                |    |
| 6.1. Conclusion.....                        | 37 |

|                            |    |
|----------------------------|----|
| 6.2. Further Research..... | 37 |
| References.....            | 38 |





## Table of Figures

|  |    |
|--|----|
| Figure 2.1 Linklist.....                             | 3  |
| Figure 2.2 Tree.....                                 | 4  |
| Figure 2.3 Priority of attributes.....               | 7  |
| Figure 2.4 Processed tree ip and tree blacklist..... | 8  |
| Figure 3.1 Incremental Model.....                    | 9  |
| Figure 4.1 Use Case Diagram.....                     | 11 |
| Figure 4.2 Class Diagram.....                        | 12 |
| Figure 4.3 PortScanner class.....                    | 13 |
| Figure 4.4 NodePath class.....                       | 13 |
| Figure 4.5 NodeMessage class.....                    | 14 |
| Figure 4.6 FileWrite class.....                      | 14 |
| Figure 4.7 Linklist class.....                       | 15 |
| Figure 4.8 NodeTree class.....                       | 15 |
| Figure 4.9 NodeIP class.....                         | 16 |
| Figure 4.10 SearchString class.....                  | 17 |
| Figure 4.11 Directory Class.....                     | 18 |
| Figure 4.12 NodeSearchResult.....                    | 19 |
| Figure 4.13 BinaryTree.....                          | 19 |
| Figure 4.14 GA class.....                            | 20 |
| Figure 4.15 FileRead2 class.....                     | 20 |
| Figure 4.16 Main class.....                          | 22 |
| Figure 5.1. Scan log.....                            | 32 |
| Figure 5.2. Scan File Trojan.....                    | 32 |
| Figure 5.3 Scan trojan rootkit.....                  | 33 |
| Figure 5.4 Scan IP.....                              | 33 |

Figure 5.5 Scan All port.....34  
Figure 5.6 Scan single port.....34  
Figure 5.7 Write to iptables (firewall).....35  
Figure 5.8 iptables before insert rule.....35  
Figure 5.9 iptables after insert rule.....36



## Table of Tables

|                                   |    |
|-----------------------------------|----|
| Table 2.1. Table calculation..... | 6  |
| Table 3.1 Project Management..... | 10 |

