UNIVERSITAS MERCU BUANA

NETWORK SECURITY MONITORING SYSTEM USING NOTIFICATION ALERTS

TUGAS AKHIR

Diajukan guna melengkapi sebagian syarat dalam mencapai gelar Sarjana Strata Satu (S1)

DisusunOleh:

Nama	**: Rachmat Muwardi**
NIM	**: 41413010013**
Program Studi	**: Teknik Elektro**
Pembimbing	**: Akhmad Wahyu Dani, S.T., M.T.**

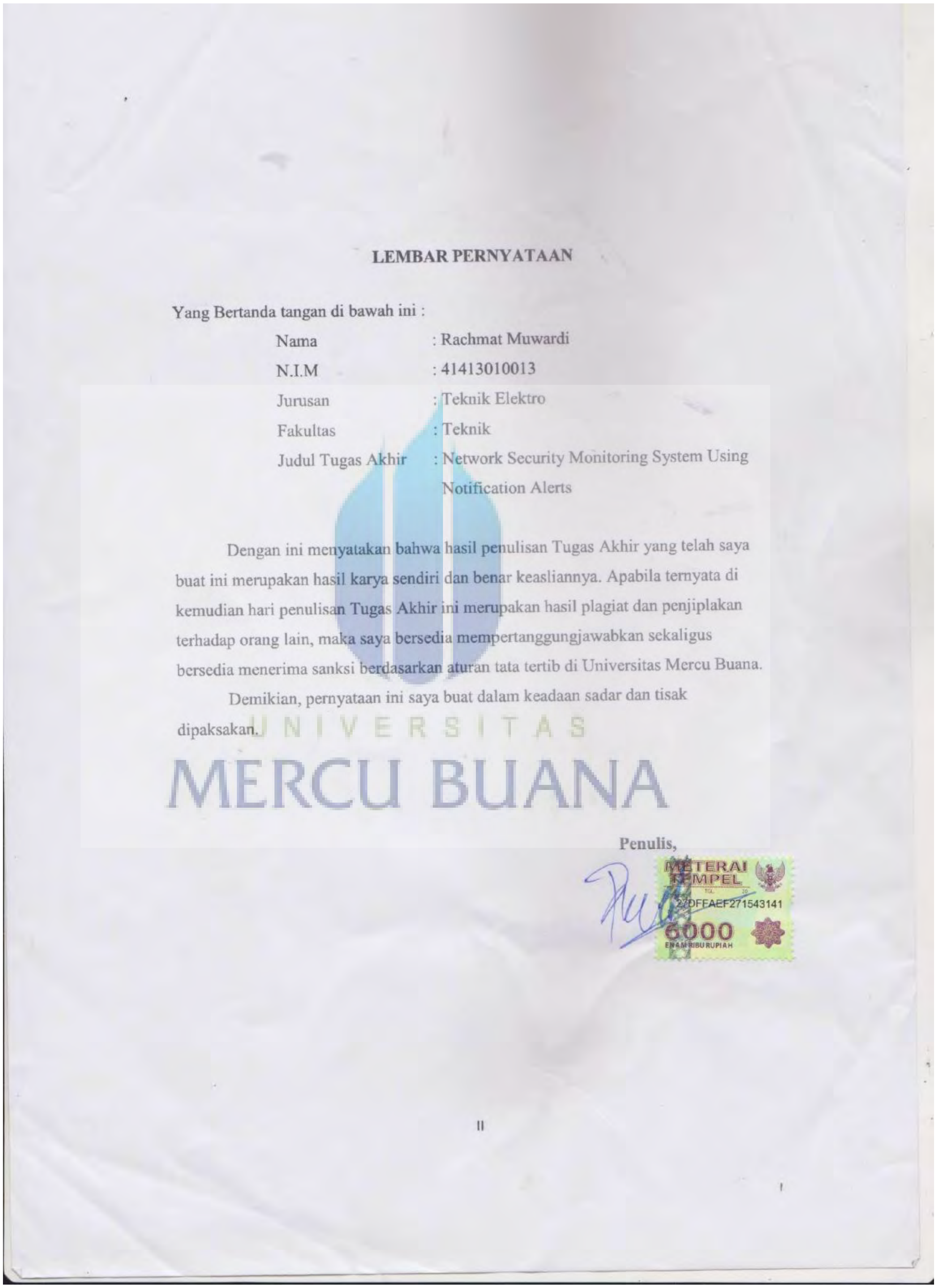
PROGRAM STUDI TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS MERCU BUANA

JAKARTA
2017

https://digilib.mercubuana.ac.id/



LEMBAR PERNYATAAN

Yang Bertanda tangan di bawah ini :

Nama	: Rachmat Muwardi
N.I.M	: 41413010013
Jurusan	: Teknik Elektro
Fakultas	: Teknik
Judul Tugas Akhir	: Network Security Monitoring System Using Notification Alerts

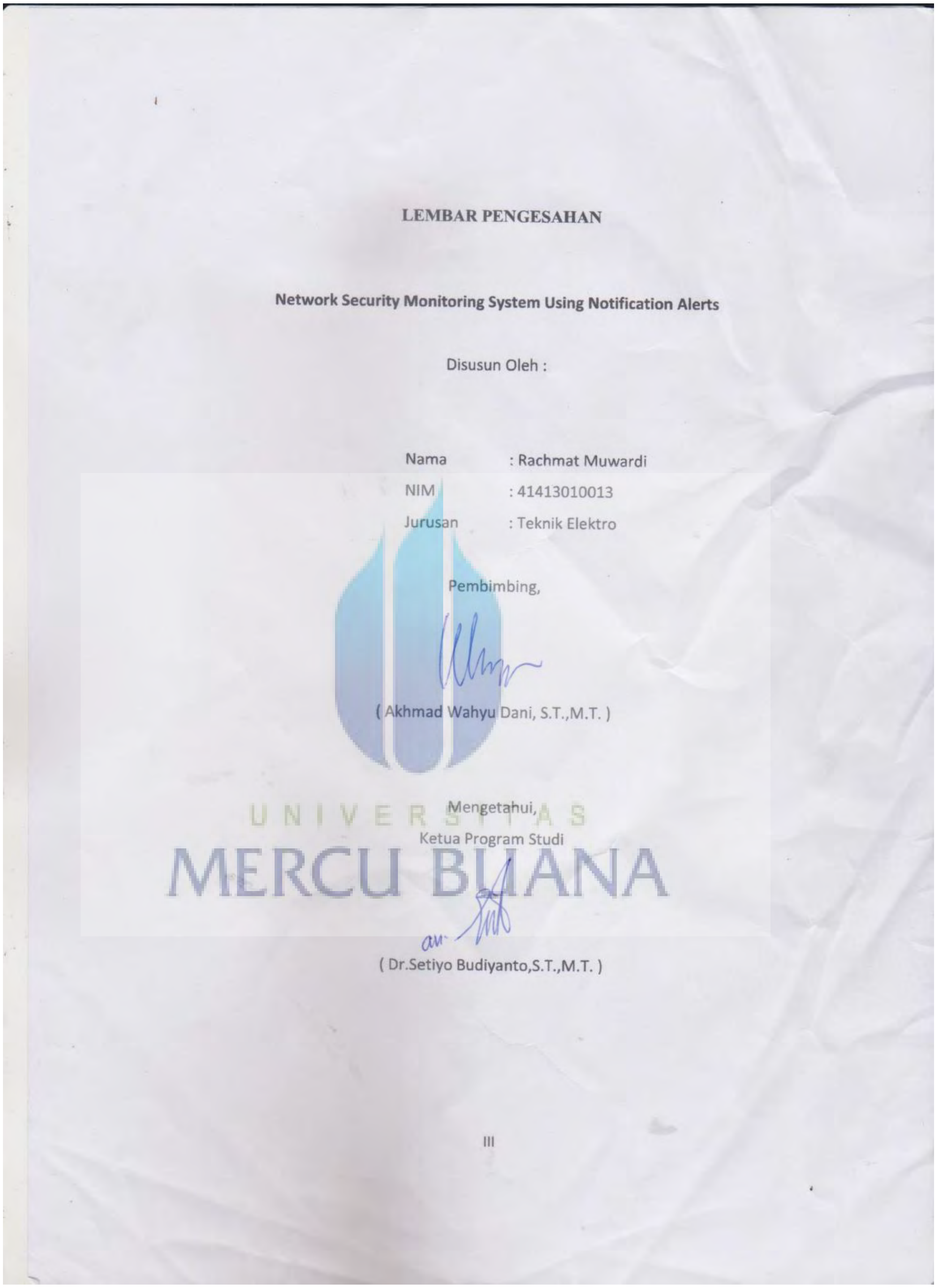
Dengan ini menyatakan bahwa hasil penulisan Tugas Akhir yang telah saya buat ini merupakan hasil karya sendiri dan benar keasliannya. Apabila ternyata di kemudian hari penulisan Tugas Akhir ini merupakan hasil plagiat dan penjiplakan terhadap orang lain, maka saya bersedia mempertanggungjawabkan sekaligus bersedia menerima sanksi berdasarkan aturan tata tertib di Universitas Mercu Buana.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tisak dipaksakan.

UNIVERSITAS
MERCU BUANA

Penulis,

METERAI TEMPEL
27DFFAEF271543141
6000
ENAM RIBU RUPIAH



LEMBAR PENGESAHAN

Network Security Monitoring System Using Notification Alerts

Disusun Oleh :

Nama : Rachmat Muwardi

NIM : 41413010013

Jurusan : Teknik Elektro

Pembimbing,

(Akhmad Wahyu Dani, S.T.,M.T.)

Mengetahui,

Ketua Program Studi

an

(Dr.Setiyo Budiyanto,S.T.,M.T.)

UNIVERSITAS
MERCU BUANA

https://digilib.mercubuana.ac.id/

KNOWLEDGMENT

Praise Alhamdulillah writer said to Allah for blessing, grace and guidance of Him, preparation of the thesis entitled “Network Security Monitoring System Using Notification Alerts” that’s one the requirements for completing the study Bachelor Program at the School Of Computer Science and Enggineering, Beijing Institute of Technology can be resolved properly.

The author realizes that this final report is far from perfect. Therefore, criticism and sugestions will always be the author is welcome. With all the limitations, the authors recognize also that this final report will not be realized without the support, guidance, and encouragement from various parties. Therefore, with all humility. Author express gratitude to:

1. Mr.Yanlong Zhai and Mr.Akhmad Wahyu Dani as the final project supervisor who never tire of giving suggestion and motivation for this project
2. Parents, brothers, sister and friend beloved who always support, pray and devote all their love the author.

In conclusion, may allah repay his kindness and always pour his mercy and guidance to us all, amen.

UNIVERSITAS MERCU BUANA

Jakarta, Jul 2017

LIST OF CONTENT

LEMBAR PERNYATAAN.. II

LEMBAR PENGESAHAN III

ACKNOWLEDGMENT IV

ABSTRACT.. V

LIST OF CONTENT...VI

LIST OF FIGURE IX

LIST OF TABLE X

CHAPTER 1 1

1.1. Project Background.. 1
1.2. Problem Statement 2
1.3. Scope of Problem 3
1.4. Research Objective 3

CHAPTER 2 4

2.1. Basic Theory.. 4
2.1.1. Understanding Intruders.. 4
2.1.2. Basic Concept of Networking Security.. 4
2.1.3. Workstation.. 6
2.1.4. Gateway 7
2.1.5. LAMP (Linux, Apache, MySQL, PHP... 7
2.1.6. IDS (Intrusion Detection System)... 8
2.1.6.1. NIDS (Network Intrusion Detection Systems) 9
2.1.6.2. HIDS (Host Intrusion Detection Systems) 9
2.2. Server 10
2.2.1. MySQL (My Structured Query Language) 10
2.2.2. Snort.. 11
2.2.3. Apache... 12
2.2.4. PHP (Hypertext Preprocessor) 13
2.2.5. Mail server... 14
2.2.6. Postfix.. 14
2.2.7. Barnyard2... 14
2.2.8. PulledPork 15
2.2.9. Snorby 15
2.3. Client 15
2.3.1. Application Services Provider... 15
2.3.2. Mail Client... 16
2.3.3. FTP (File Transfer Protocol) 16

UNIVERSITAS MERCU BUANA

2.4. Threat 17
2.4.1. Port Scanner 17
2.4.2. Teardrop Attack 18
2.4.3. Spoofing Attack 18
2.4.4. Land Attack 18
2.4.5. Smurf Attack 19
2.4.6. UDP Attack 19
2.4.7. ICMP Flood 20
2.5. Support 20
2.5.1. Microsoft Visual Studio 2017 20
2.5.1.1. Microsoft Visual C# 21
2.5.2. C/C++ Language On Ubuntu 21
2.5.3. Database 23
2.5.4. Filezilla 23
2.5.5. Secure Shell (SSH) 24
2.5.6. Nmap 24
2.5.7. Ping Attack 25

CHAPTER 3 27
3.1. System Analysis 27
3.1.1. Problem Analysis 27
3.1.2. Requirement Analysis 29
3.2. Workflow System 30
3.3. System Design 31
3.3.1. Designing Use Case Diagram 31
3.3.1.1. Snorby 33
3.3.1.2. Snort 34
3.3.1.3. Data Processor 35
3.3.1.4. Email Alert 36
3.3.1.5. Application Service (Client) 37
3.3.2. Designing Activity Diagram 37
3.3.2.1. Snorby Activity Diagram 38
3.3.2.2. Snort Activity Diagram 39
3.3.2.3. Data Processor Activity Diagram 40
3.3.2.4. Mail Alert Activity Diagram 41
3.3.2.5. Application Service (Client) Activity Diagram 42
3.3.3. Designing Sequence Diagram 43
3.3.3.1. Snorby Sequence Diagram 43
3.3.3.2. Snort Sequence Diagram 44
3.3.3.3. Data Processor Sequence Diagram 45
3.3.3.4. Mail Alert Sequence Diagram 46
3.3.3.5. Application Service (Client) Sequence Diagram 47

UNIVERSITAS
MERCU BUANA

https://digilib.mercubuana.ac.id/

3.4. Designing Interfaces 48

3.4.1. Snorby Interface Design.. 49

3.4.1. Application Service (Client) Interface Design.. 52

CHAPTER 4 53

4.1. System Implementation.. 53

4.1.1. Implementation IDS.. 53

4.1.1.1. Install Snort.. 54

4.1.1.2. Configure Snort.. 56

4.1.1.3. Install Branyard2.. 57

4.1.1.4. Install and Configure Snorby 59

4.2. Fuctionality Testing.. 59

4.2.1. Environmental Testing 60

4.2.2. Scenario Testing.. 61

4.2.3. Test Result 62

CHAPETER 5.. 68

5.1. Conclusion 68

5.2. Recommendation 68

REFERENCES 69

Sourch Code..

UNIVERSITAS
MERCU BUANA

LIST OF FIGURE

Figure 2.1. Topological layout of described network..6
Figure 3.1. The Process monitoring...30
Figure 3.2. Aplication use case...32
Figure 3.3. The Snorby Activity Diagram...38
Figure 3.4. The Snort Activity Diagram 39
Figure 3.5. The Data Processor Activity Diagram 40
Figure 3.6. The Mail Alert Activity Diagram 41
Figure 3.7. The Application Service (Client) Activity Diagram.......................................42
Figure 3.8. The Snorby Sequence Diagram 43
Figure 3.9. The Snort Sequence Diagram 44
Figure 3.10. The Data Processor Sequence Diagram...45
Figure 3.11. The Email Alert Sequence Diagram..46
Figure 3.12. The Application Service (Client) Sequence Diagram 47
Figure 3.13. Run Snorby 49
Figure 3.14. Home Page Interface Snorby 50
Figure 3.15. Sensor Interface Snorby..51
Figure 3.16. Application Service (Client) 52
Figure 4.1. Snort Version 56
Figure 4.1. Test get data with Application Service 66
Figure 4.1. Test Result Email Alert...67

UNIVERSITAS
MERCU BUANA

https://digilib.mercubuana.ac.id/

LIST OF TABLE

Table 3.1. The Snorby Use case..33
Table 3.2. The Snort Use case 34
Table 3.3. Data Processor Use case...35
Table 3.4. Email Alert Use case..36
Table 3.5. Application Service (Client) Use case 37
Table 4.1. Install Packet Support IDS..53
Table 4.2. Install Snort 55
Table 4.3.Configure Snort..57
Table 2 4 Install Branyard2 58
Table 4.5. Install and Configure Snorby..59
Table 4.6. Threat Scenario Testing...61
Table 4.7. Server Scenario Testing 62
Table 4.8. Threat Scenario Testing...62
Table 4.9. Threat Test Result..62
Table 4.10. Server Test Result 64
Table 4.11. Client Test Result 66

UNIVERSITAS
MERCU BUANA

https://digilib.mercubuana.ac.id/