WINDOW HARDENING FOR WINDOW SERVER 2003

GUI KHENG LENG

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS TESIS

JUDUL: WINDOW HARDENING FOR WINDOW SERVER 2003

SESI PENGAJIAN: 2009/2010

Saya GUI KHENG LENG

(HURUF BESAR)

mengaku membenarkan tesis (PSM/~~Sarjana/Doktor Falsafah~~) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

______	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
______	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)
/	TIDAK TERHAD	

(TANDATANGAN PENULIS)
Alamat tetap: No 7, Jln Impian 1,
Taman Impian, Pasir Tuntong, 45700
Bukit Rotan, Selangor
Tarikh: 28 June 2010

(TANDATANGAN PENYELIA)
DR. SUHAIMI BIN BASRAH
(Nama Penyelia)
Tarikh: 28/06/10

CATATAN: *Tesis dimaksudkan sebagai Laporan Akhir Projek Sarjana Muda (PSM)
** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

WINDOW HARDENING FOR WINDOW SERVER 2003

GUI KHENG LENG

This report is submitted in partial fulfillment of the requirements for the Bachelor of Computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2010

DECLARATION

I hereby declare that this project report entitled

WINDOW HARDENING FOR WINDOW SERVER 2003

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : ______________________ Date: 18/6/2010

(GUI KHENG LENG)

SUPERVISOR : ______________________ Date: 28/06/10

(DR. SUHAIMI BIN BASRAH)

DEDICATION

To my family especially to my beloved mom and dad who always give me encouragement to finish this project

ACKNOWLEDGEMENT

I thank God, for with Him, nothing is impossible.

I would like to express my gratitude to my supervisor Dr. Suhaimi bin Basrah for his guidance and advice throughout the course of my studies. His close supervision and guidance in thesis writing methodology and system development has been valuable. I am also very grateful to my evaluator, En.Mohammad Radzi Motsidi for his suggestions and feedback during the evaluation.

I would also like to thank to my entire friends, without their helping, support and valuable option during the project, I would never been able to accomplish my project. Also not forget to any individual that have not mention here but has contributed to this project. To all of them, I only can say very much thank you for their help and support.

Last but not least, I would like to thank to my family for their understanding, encouragement and support towards the completion of my project.

ABSTRACT

Nowadays, most of our routine tasks are no longer done by human but computer has taken the place. Computers are serving as important data processing devices and data storage. However, there is an issue that occurs, is it the computers are secured?

A secure computer can prevent unauthorized access and secure sensitive information from being stolen. However, there are many people do not know how to secure their computer. Local Security Policy refers to a collection of settings relating to the security of computers that running Microsoft Windows OS. Based to the settings, we can determine the window is hardening or vulnerability to be attacked.

Currently, the Local Security Settings is checked manually and it is time-consuming. Furthermore, there are many users do not know how to check the settings. Therefore, the proposed system shall solve all of the limitations above as the proposed system can check the settings and compare with benchmarks automatically. Then, users can base on the checking and take necessary precaution.

ABSTRAK

Pada zaman sekarang, semakin banyak kerja harian telah dilakukan menggunakan komputer. Komputer dilayani sebagai satu peranti pemprosesan data dan simpanan data. Namum begitu, satu isu telah dibangkitkan, adakah komputer tersebut selamat?

Komputer yang selamat dapat menghalang pengguna yang tiak sah dan melindungi data yang penting. Namum begitu, kebanyakan pengguna tidak tahu melindungi komputernya. *Local Security Policy* adalah koleksi tatacara bagi keselamatan komputer. Berasaskan tatacara tersebut, kita dapat menentukan komputer tersebut sleamat atau senang diserang.

Pada masa sekarang, *Local Security Settings* adalah disemak secara manual dan ini amat memakan masa. Selanjutnya, ada banyak pengguna yang tidak tahu menyemak tatacara tersebut. Oleh demikian, satu sistem akan dibangunkan untuk menyelesaikan masalah tersebut. Sistem tersebut akan menyemak tatacara dan membandingkan dengan benchmark secara automatik. Maka, pengguna dapat mengambil tindakan pencegahan yang diperlukan.

TABLE OF CONTENTS

CHAPTER	SUBJECT	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENTS	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xii
	LIST OF FIGURES	xiv
	LIST OF ABBREVIATIONS	xvi
	LIST OF ATTACHMENTS	xviii
CHAPTER I	INTRODUCTION	
	1.1 Project Background	1
	1.2 Problem Statements	2
	1.3 Objective	2
	1.4 Scope	2

1.5 Project Significant 3
1.6 Expected Output 3
1.7 Conclusion 4

CHAPTER II LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction 5
2.2 Literature Review 5
2.2.1 Domain 5
2.2.2 Keyword 6
2.2.3 Previous Research 6
2.2.3.1 First Research: Password Auditing Applications 6
2.2.3.1.1 LC5 7
2.2.3.1.2 SAMInside 7
2.2.3.1.3 John the Ripper 8
2.2.3.1.4 Crack 8
2.2.3.2 Second Research: Vulnerability Profile for Linux 8
2.2.3.3 Third Research: PCChecker: Hardening Window Security Configurations 10
2.2.3.4 Comparisons of Research 12
2.2.4 Facts and Findings 13
2.2.4.1 Methodologies 13
2.2.4.2 Comparison of Methodologies 17
2.2.4.3 Databases 18
2.2.4.4 Comparison of Databases 18
2.2.4.5 Scripting Languages 20
2.2.4.6 Comparison of Scripting Languages 20

2.3 Proposed Solution 21

2.3.1 Project Methodology 21

2.3.1.1 Planning 22

2.3.1.2 Analysis 23

2.3.1.3 Design 23

2.3.1.4 Implementation 24

2.3.1.5 Testing 24

2.4 Project Schedule and Milestones 24

2.5 Conclusion 24

CHAPTER III ANALYSIS

3.1 Introduction 26

3.2 Problem Analysis 26

3.2.1 Analysis of Current System 26

3.2.2 Problems of Current System 31

3.3 Requirement Analysis 33

3.3.1 Data Requirement 33

3.3.2 Functional Requirement 34

3.3.3 Non-functional Requirement 37

3.3.3.1 Operating System 37

3.3.3.2 Performance 37

3.3.4 Others Requirement 37

3.3.4.1 Software Requirement 38

3.3.4.2 Hardware Requirement 38

3.4 Conclusion 39

CHAPTER IV DESIGN

4.1 Introduction 40

4.2 High-Level Design 40

4.2.1 System Architecture 40

4.2.2 Interaction Diagram 42

4.2.3 User Interface Design 42

4.2.3.1 Navigation Design 43

4.2.3.2 Input Design 44

4.2.3.3 Output Design 44

4.2.4 Database Design 45

4.2.4.1 Conceptual and Logical Database Design 45

4.3 Detailed Design 46

4.3.1 Software Design 46

4.3.2 Physical Database Design 47

4.4 Conclusion 47

CHAPTER V IMPLEMENTATION

5.1 Introduction 48

5.2 Software Development Environment Setup 48

5.3 Software Configuration Management 49

5.3.1 Configuration environment setup 49

5.3.1.1 Microsoft Access ODBC Data Source 50

5.3.2 Version Control Procedure 52

5.4 Implementation Status 53

5.5 Conclusion 54

CHAPTER VI TESTING

6.1 Introduction 55

6.2 Test Plan 55

6.2.1 Test Organization 56

6.2.2 Test Environment 56

6.2.3 Test Schedule 57

6.3 Test Strategy 58

6.3.1 Classes of tests 59

6.3.1.1 Unit Testing 59

6.3.1.2 Functionality Testing 59

6.3.1.3 User Acceptance Testing 60

6.3.1.4 Error Handling Testing 60

6.3.1.5 Integration Testing 60

6.4 Test Design 60

6.4.1 Test Description 61

6.4.2 Test Data 63

6.5 Test Results and Analysis 66

6.5.1 Account Policies Setting 66

6.5.2 Local Policies Setting 67

6.6 Conclusion 67

PTER VII PROJECT CONCLUSION

7.1 Observation on Weakness and Strengths 68

7.1.1 Strengths 68

7.1.2 Weaknesses 69

7.2 Propositions for Improvement 69

7.3 Contribution 70

7.4 Conclusion 70

References 71

Bibliography 73

Appendix A – Gantt Chart 74

Appendix B – Entity Relationship Diagram 75

Appendix C – Data Dictionary 76

Appendix D – Software Design 78

Appendix E – Physical Database Design 79

Appendix F – User Manual 80

LIST OF TABLES

TABLE	TITLE	PAGE
1.1	Checklist in Account Policies and Local Policies	3
2.1	Comparison of Previous Research	12
2.2	Comparison of Methodologies	17
2.3	Comparison of Databases	18
2.4	Comparison of Scripting Languages	20
3.1	CIS Membership Categories	31
3.2	Data Dictionary for Password Policy Table	34
3.3	List of Software Requirement	38
3.4	List of Hardware Requirement	39
5.1	List of Version Control	53
5.2	Implementation status of Window Hardening for Window Server 2003	54
6.1	Hardware and software requirement for testing environment	57

6.2 **Test Schedule of Window Hardening for Window Server 2003** **58**

6.3 **Test Description for Account Policies Setting** **61**

6.4 **Test Description for Local Policies Setting** **62**

6.5 **Test Description for Account Policies Status** **62**

6.6 **Test Description for Local Policies Status** **63**

6.7 **Test Data for Account Policies Setting** **63**

6.8 **Test Data for Local Policies Setting** **65**

6.9 **Test Result for Account Policies Setting** **66**

6.10 **Test Result for Local Policies Setting** **67**

LIST OF FIGURES

DIAGRAM	TITLE	PAGE
2.1	Damages due to vulnerability of vanilla	9
2.2	Effects of security enhancements on damages and overall system vulnerability	10
2.3	PCChecker Module Structure	11
2.4	PCChecker Result	12
2.5	Classical Waterfall Model	14
2.6	Iterative Waterfall Model	15
2.7	Prototyping Model	15
2.8	Spiral Model	16
2.9	Project Methodology - Iterative Waterfall Model	22

3.1 CIS-CAT Interfaces 27

3.2 Select a benchmark Interface 27

3.3 Select Benchmark & Profile Interface 28

3.4 Run Benchmark Interface 29

3.5 Browse Result Interface 30

3.6 Summary of Results Interface 31

3.7 The Flowchart of The Proposed System 35

3.8 The Use Case of the Proposed System 36

Layered Architecture of Proposed System 41

Interaction Diagram for a Security Checking 42

Navigation Design of The Design 43

File Option of The Proposed System 44

Password Policy 45

Software Development Environment 49

LIST OF ABBREVIATIONS

CIS	-	Center for Internet Security
ICT	-	Information Communications Technology
OS	-	Operating System
SANS	-	SysAdmin, Audit, Network, Security
DAC	-	Discretionary access control
LSM	-	Linux Security Modules
CVSS	-	Common Vulnerability Scoring System
SDM	-	Software Development Methodology
RDBMS	-	Relational Database Management System
VBScript	-	Visual Basic Scripting Edition
WSH	-	Windows Script Host
IIS	-	Internet Information Services
JVM	-	Java Virtual Machine
ERD	-	Entity Relation Diagram
LDM	-	Logical Data Model
CIS-CAT	-	CIS Configuration Audit Tool
CPU	-	Central Processing Unit

SC	-	Security Checking

LIST OF ATTACHMENTS

APPENDIX	TITLE	PAGE
A	Gantt Chart	74
B	Entity Relationship Diagram (ERD)	75
C	Data Dictionary	76
D	Software Design	78
E	Physical Database Design	79
F	User Manual	80

CHAPTER I

INTRODUCTION

1.1 Project Background

Information Security is an important issue in network. Information Security is defined the protection of information and the systems and hardware that use, store and transmit that information. A secure environment can prevent and protect sensitive information such as credit card information or password from being stolen by unauthorized people. However, most of the people do not know how to secure their information or computer. This phenomena leads to security threat, such as hacking.

Center for Internet Security (CIS) is non-profit enterprises that help organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls. CIS provide benchmarks, information, suggestions or ideas to organizations attempting to improve the security of their network, systems or devices.

The benchmark is a recommended technical control rules or values that use for hardening operating systems, middleware, software applications and network devices. Users can use these benchmarks to enhance their personal network security or computer. Basically, the benchmarks are described in terms of updating the Local Security Policy. The Local Security Policy Editor is located in the Administrative Tools menu. Users manually checking the settings in Local Security Policy and compare it with the benchmarks. After that, users will be able to determine whether the system is vulnerable to attack or not.

All of the checking and comparing activities are done by manually is time consuming. So, a system will be developed to check the settings in Local Security Policy and compare it with benchmarks automatically.

1.2 Problem Statements

Currently, there is no any system that can automatically check the security settings. Thus, users will waste time in checking and comparing the settings in Local Security Policy. Besides, Local Security Policy consists of many sub policy where users does not know how to check the settings. Even they know how to check the settings, they also face difficulties when want to configure it.

1.3 Objective

The objectives of this project are as follows:

- To develop a system that can check and compare the settings in Local Security Policy with benchmark automatically.
- To improve the safety level of the system
- To instruct users how to secure their system

1.4 Scope

The system is developed to check and compare the settings in Local Security Policy. Basically, the system is build by using the JAVA and the platform for using the system is focus on Window Server 2003 Standard Edition. The settings in Local Security Policy that will be check is the checklists that locate in Local Policies and Account Policies. The target user of the system will be everyone.

1.5 Project Significance

At the end of the project, users will know how to secure their computer. This indirectly can improve the safety level of the computer and prevent the happen of security threat.

1.6 Expected Output

By completing this project, a system will be developed to check the settings in Local Security Policy and compare the current settings with the benchmark settings automatically. If the setting is match, the status is mark as Pass while the setting is no match, the status is mark as Fail. Table 1.1 below show that the part of the checklists in Account Policies and Local Policies.

Table 1.1: Checklists in Account Policies and Local Policies

Local Security Setting	Benchmark	Status
1. Account Policies		
1.1 Password Policy		
1.1.1 Enforce password history	24 passwords remembered	Pass
1.1.2 Maximum password age	42 days	Pass
1.1.3 Minimum password age	1 day	Fail
1.2 Account Lockout Policy		
1.2.1 Account lockout duration	15 minutes	Fail

1.2.2 Account lockout threshold	15 attempts	Fail
2. Local Policies		
2.1 Audit Policy		
2.1.1 Audit account logon events	Success and Failure	Pass
2.1.2 Audit account management	Success and Failure	Fail
2.2 User Rights Assignment		
2.2.1 Access this computer from the network	<Not Defined>	Fail
2.2.2 Act as part of the operating system	<None>	Fail
2.3 Security Options		
2.3.1 Accounts: Administrator account status	<Not Defined>	Fail
2.3.2 Accounts: Guest account status	Disabled	Pass

1.7 Conclusion

As a conclusion, the system that will be developed is able to solve the problem about the time consuming in checking and comparing the settings in Local Security Policy. The system also able to improve the secure state of a computer and every user are becomes the security aware to improve the safety level of the internet.

In the next chapter, the literature review and project methodology chapter are going to focus about the research that related in the project. Besides that, project methodology, project schedule and milestone are also will be explain in next chapter.