COMPARING THE VULNERABILITY OF PASSWORD SECURITY ON WINDOWS XP PROFESIONAL AND RED HAT LINUX 9

NORKHUSHAINI AWANG

UNIVERSITI UTARA MALAYSIA
2004

JABATAN HAL EHWAL AKADEMIK
(*Department of Academic Affairs*)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

NORKHUSHAINI BT. AWANG

calon untuk Ijazah
(candidate for the degree of) **MSc. (Information Technology)**

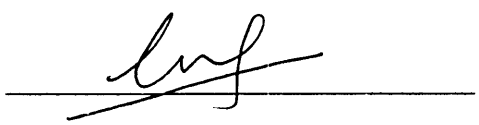
telah mengemukakan kertas projek yang bertajuk
(has presented his/ her project paper of the following title)

COMPARING THE VULNERABILITY OF PASSWORD SECURITY ON WINDOWS XP PROFESSIONAL AND RED HAT LINUX 9

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the filed is covered by the project paper).

Nama Penyelia Utama
(Name of Main Supervisor): **MRS. NAFISHAH OTHMAN**

Tandatangan
(Signature) : 

Tarikh
(Date) : 10/11/04

COMPARING THE VULNERABILITY OF PASSWORD SECURITY ON WINDOWS XP PROFESIONAL AND RED HAT LINUX 9

Declaration of Author's Right

NORKHUSHAINI AWANG (83394)

November 2004

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor or, in thesis absence, by the Dean of the Faculty of Information Technology. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be of any material form my thesis.

Request for permission to copy or to make other use of material in this thesis, in whole or in part, should be addressed to:

Dean of the Faculty of Information Technology
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darulaman

Abstrak

Keselamatan komputer merupakan satu elemen penting yang mesti diambil kira di dalam sesuatu rangkaian komputer. Perkara asas di dalam keselamatan komputer adalah keselamatan katakunci yang terdapat dalam sesuatu sistem pengoperasian. Kajian yang dilakukan ini memfokuskan kepada sistem pengoperasian Windows XP Professional dan Red Hat Linux 9 kerana kedua-dua sistem pengoperasian ini popular digunakan oleh pengguna di Malaysia. Tujuan utama kajian ini adalah untuk mengenalpasti kelemahan di dalam keselamatan katakunci yang terdapat di dalam kedua-dua sistem pengoperasian ini. Dua komputer telah di sambungkan untuk mensimulasikan serangan seperti di dalam rangkaian komputer. Sistem pengoperasian yang digunakan iaitu Windows XP Professional dan Red Hat Linux 9 telah dikonfigurasikan dengan *firewall* yang terdapat didalamnya. Ini adalah untuk memastikan kedua-dua sistem pengoperasian ini dilengkapi dengan tahap keselamatan yang tinggi. Daripada kajian yang telah dibuat didapati keselamatan katakunci pada kedua-dua sistem pengoperasian ini mudah dicerobohi walaupun telah dikonfigurasikan dengan *firewall*. Oleh itu, beberapa langkah mesti di ambil untuk memastikan keselamatan rangkaian komputer kita bebas daripada pengodam.

Abstract

Computer security is an important element that should be consider in computer networking. The basic element in computer security is password security in operating systems. This research focus on Windows XP Professional and Red Hat Linux 9 operating systems because both of these platform is popular used by Malaysian users. The main objective of this research is to identify the vulnerability of password security in both operating systems. Two computers have been connected to stimulate the attacking scenario such as in computer network. Both operating systems which is Windows XP Professional and Red Hat Linux 9 have been configured with firewall that come with the system. This is to ensure that both operating systems is prevent with high level security. From the research study, found that password security on both platform is easy to be crack even firewall is configure earlier. Therefor, some steps should be taken to ensure security in computer network is zero from hackers.

ACKNOWLEDGMENTS

BISMILLAHIRRAHMANIRRAHIM

In the name of ALLAH, the most gracious and the most merciful

Alhamdulillah, thanks to the Almighty for blessing me with strength and courage to complete this thesis. In the midst of preparing and completing this thesis, I have the privilege of obtaining assistance and guidance from various sources. Therefore, I would like to express my deepest appreciation to those involved in this thesis.

First and foremost, I would like to thank my beloved husband Mohamad Yusof B. Darus for the continue support and always give encouragement to me to finish this research. I also want to thank my supervisor Puan Nafishah Bt. Othman in supervised me and giving suggestion for me in prepared this research project. All of her contribution will kept in my mind and in my heart, will be remembered, as it is such a priceless effort for me.

Last but not least, I would like to express my appreciation to my beloved parents Awang B. Mamat and Noraini Mohamad Noor as without their moral support, I would not make it until today. For those whom not stated here, I would like to thank for their help, friendship and countless support to me. May ALLAH S.W.T. bless all of them for their support and kindness.

Thank you again.

Table of Contents

Permission To Use	i
Abstrak	ii
Abstract	iii
Acknowledgements	iv
Table of Contents	v
List of Figures	vii
List of Tables	viii
List of Abbreviations	ix
Chapter 1: Introduction	
1.0 Research Background	1
1.1 Problem Statement	6
1.2 Research Objectives	7
1.3 Scope	7
1.4 Significance Of Study	8
1.5 Thesis Structure	9
Chapter 2: Literature Review	
2.0 Introduction	10
2.1 Windows XP Professional	11
2.2 Red Hat Linux 9	14
2.3 Password Security	17
2.4 Previous Study on Password Security	20
2.5 Research Methodology	23
2.6 Conclusion	27
Chapter 3: Methodology	
3.0 Introduction	28
3.1 Phase 1- Data Collection	30
3.2 Phase 2- Configuration	31
3.2.1 Installation of Windows XP Professional	31
3.2.2 Installation of Red Hat Linux 9	31
3.2.3 LAN Configuration	31
3.2.4 Firewall Configuration	32
3.2.4.1 Setup Firewall in Windows XP Professional	32
3.2.4.2 Setup Firewall in Red Hat Linux 9	37
3.3 Phase 3- Testing	38
3.3.1 Crack Windows XP Professional Computer	40
3.3.2 Crack Red Hat Linux 9 Computer	45
3.4 Phase 4- Verification	54
3.5 Conclusions	55

Chapter 4: Findings
4.0 Introduction 56
4.1 Guideline in Secure the Network 56
4.1.1 An Enforcement of Password Policy 57
4.1.2 Smartcards and Tokens 58
4.1.3 Biometrics 60
4.1.4 Shadowing the Passwords Files 62
4.2 Conclusion 63

Chapter 5: Conclusion And Recommendation
5.0 Introduction 64
5.1 Recommendations 65
5.2 Limitations 65

References 66

Appendices
Appendices 1: Steps to Install Windows XP Professional 69
Appendices 2: Steps to Install Red Hat Linux 9 74

List of Figures

2.1: Relationship between security, convenience, and cost 19
2.2: Soft Systems Methodology 24
2.3: Framework Of Network Rating Model (NRM) 25
2.4: Research Model Adapt From Network Rating Model (NRM) 27
3.1: LAN Configuration 32
3.2: My Network Places 33
3.3: View Network Connections 33
3.4: Network Bridge 34
3.5: Network Bridge Properties 35
3.6: Internet Connection Firewall 35
3.7: Network Bridge Properties 36
3.8: Network Connections 36
3.9: Customize firewall setting 38
3.10: Model of Security Testing 40
3.11: CAP and Run Command 41
3.12: Tools menu 42
3.13: Sharing files in can be access 43
3.14: Run the Command 44
3.15: Open Strategies Management File 45
3.16: Start button 46
3.17: Run Command: regedt32 46
3.18: Find the requiresignorseal file 47
3.19: Default value in dword: 00000001 48
3.20: Change the dword value 48
3.21: Changing have been made 49
3.22: End setup 49
3.23: Test cracking the Red Hat Linux 9 50
3.24: View workgroup computers 50
3.25: View of samba server (Syah) and syah(Zaha) machine 51
3.26: To test either success or not 52
3.27: Display folder satu 52
3.28: Retrieve file from folder satu 53
3.29: Open smb.conf file 54

List of Tables

3.1: Hardware and Software Requirement 30

List of Abbreviations

ACL	Access Control List
CCT	Comparing Caching Techniques
CD-ROM	Compact Disc-Read-Only Memory
CEO	Chief Executive Officer
Corp.	Corporation
DoS	Denial of Service
FTP	File Transfer Protocol
GAO	General Accounting Office
ICF	Internet Connection Firewall
ID	Identity
IP	Internet Protocol
ISECOM	Security and Open Methodologies
IT	Information Technology
LAN	Local Area Network
MB	Megabyte
NIST	National Institute for Standards and Technology
NRM	Network Rating Model
NSA	National Security Agency
OS	Operating System
PC	Personal Computer
PIN	Personal Identification Number
RAM	Random Access Memory
RHEL	Red Hat Enterprise Linux
SA	System Administrator
SANS	SysAdmin Audit Network Security
SP2	Service Pack 2
SSM	Soft Systems Methodology
TCP/IP	Transfer Control Protocol/Internet Protocol
UTP	Unshield Twisted-Pair

CHAPTER 1

INTRODUCTION

1.0 Research Background

Network security is a complicated subject, previously only carried out by well-trained and experienced experts. However, as more and more people become wired, an increasing number of people need to understand the basics of security in a networked world. A dedicated attacker trying a variety of remote commands until he or she successfully cracks the system password. Instead, most attacks today are performed using automated tools, which attempt to exploit known vulnerabilities in various operating system and applications. The key to network security can be found in understanding the choices and strategies available to the building blocks of network security. The most basic building block to any security model is user authentication. User authentication allows for verification that the user is who they say they are; therefore it gives them the ability to regulate that gains access to the network.

Password and user account exploitation is one of largest issues in network security. Attacks on a company or organization's computer systems take many

The contents of the thesis is for internal user only

REFERENCES

Beaver K. & McClure S. (2004) *Hacking For Dummies*. United States of America: Hungry Minds

Bolzern M. (2000, September). The Duality of Microsoft's Position On Linux. System Development, pp. 94-96

BrainWave Consulting (2004). *Why Is System & Network Security Important?*. Retrieved August 2, 2004, from http://www.ultratech-llc.com/BrainWave/

Cole E. (1999). *Hackers Beware*. United States of America: New Riders Publishing

Couprie D., Goodbrand A., Li B. & Zhu D. (1996) *Soft Systems Methodology*. Retrieved July 10, 2004, from http://sern.ucalgary.ca

David a. Kelly (July/August 2004) Oracle Magazine Volume XVIII Number 4 *Linux-A Hit with enterprise of all sizes and a natural for low-cost cluster*

Donald L. & Chellis J. (2002) . *MCSE: Windows XP Professional Study Guide*. New York: Sybex

Dictionary Online, Retrieved Jun 20, 2004, from http://www.m-w.com

Enterprise Business Solutions: Solving Password Management Challenges For The Technologies Sector (2004) Retrieved August 20, 2004, from http://www.protocom.com/ whitepapers/solutions_technologies.pdf

Fisher D. (2003) *Study Reveals Bad Password Habits*. Retrieved September 1, 2004, from http://searchsecurity.techtarget.com

Fisher K. (2004). *Linux Servers Targeted More Often For Attacks.* Retrieved August 10, 2004, from http://arstechnica.com/news/posts/1077304227.html

Grant R. (2004). *Linux for Non-Geeks: A Hands-On, Project-Based, Take-It-Slow Guidebook.* United States of America: No Starch Press

LeBlanc D.A., Hoag M. & Blomquist E. (2001). *Linux for Dummies* (3rd ed.). United States of America: Hungry Minds

Marina M., Rosslina H. & Siti Zaleha M. (2002) *Pengendalian Sistem Pengoperasian.* Malaysia : Dewan Bahasa dan Pustaka

Mary E. Behr (2001) *The Cracked and the Crackers Respond.* Retrieved July 23, 2004, from www.pwcrack.com

Robert J. Shimonski (2002). *Introduction to password cracking.* Retrieved July 23, 2004, from http://www.alphaworks.ibm.com/developerworks/ratings.nsf/RateArticle?CreateDocument

Schenk T. (2004). *Leading Universities Around the World Choose Red Hat Academic Solutions for Servers and Clients.* Retrieved July 20, 2004, from http://www.redhat.com/solutions/industries/education/

Siever E., Figgins S. & Weber A. (2003) *Linux in a Nutshell* (4th ed.). United Kingdom:O'Reilly

Stanley H. Kremen. (1998). *Apprehending The Computer Hacker: The Collection and Use of Evidence.* Retrieved August 23, 2004, from http://www.shk-dplc.com/cfo/articles/hack.htm

United States General Accounting Office (1996). *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*. Retrieved August 10, 2004, from http://www.fas.org/irp/gao

Wong L.C. (2004, July 27). The Star InTech pp. IT8

Zviran M., Haga W.J. (1993): *A Comparison of Password Techniques for Multilevel Authentication Mechanisms*. The Computer Journal, 36 pp. 227-237