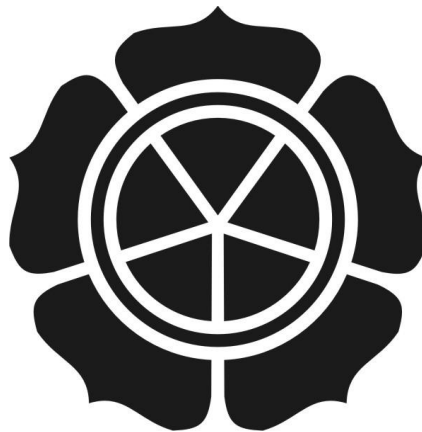


ANALISIS WINDOWS SECURITY INTERNAL

SKRIPSI



Disusun oleh :

Bayu Sigit Pambudi

05.11.0797

JURUSAN TEKNIK INFORMATIKA

**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM**

YOGYAKARTA

2010

ANALISIS WINDOWS SECURITY INTERNAL

Skripsi

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada Jurusan Teknik Informatika



Disusun oleh :

Bayu Sigit Pambudi

05.11.0797

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM**

YOGYAKARTA

2010

PERSETUJUAN

SKRIPSI

Analisis Keamanan Internal Windows

yang dipersiapkan dan disusun oleh

Bayu Sigit Pambudi

05.11.0797

telah disetujui oleh dosen pembimbing skripsi
pada tanggal 26 January 2010

Dosen Pembimbing,



Melwin Syafrizal, S.Kom, M.Eng

NIK. 190302098

PENGESAHAN

SKRIPSI

Analisis Keamanan Internal Windows

yang dipersiapkan dan disusun oleh

Bayu Sigit Pambudi

05.11.0797

telah diperthankan di depan Dewan Penguji
pada tanggal 17 Maret 2010

Susunan Dewan Penguji

Nama Penguji

M. Rudyanto Arief, M.T

NIK. 190302098

Sudarmawan, M.T

NIK. 190302035

Melwin Syafrizal, S.Kom, M.Eng

NIK. 190302105

Tanda Tangan

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
tanggal 4 Mei 2010

KEJURU STMIK AMIKOM YOGYAKARTA



Prof. Dr. M. Suvanto, MM

NIK. 190302001

PERNYATAAN

Saya yang bertanda tangan dibawah ini menyatakan bahwa, skripsi ini merupakan hasil karya saya sendiri (ASLI), dan isi di dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 15 April
2010

Bayu Sigit Pambudi
05.11.0797

KATA PENGANTAR

Windows adalah sistem operasi yang paling banyak digunakan karena kemudahan untuk mengoperasikannya. Perkembangan IT pada masa sekarang telah banyak menemukan kelemahan keamanan pada *sistem operasi Windows* hal ini memaksa *Microsoft* sebagai pihak pembuat serta pengembang *Windows* untuk melakukan perbaikan keamanan pada *Sistem Operasi Windows* yang mereka ciptakan.

Keamanan *Windows* tidak hanya untuk menunjukkan *authenticate user* tapi juga untuk menunjukkan *authorize* akses mereka. *Scenarios* umum yang menyebabkan kita membutuhkan lebih banyak keamanan diantaranya:

- Bagaimana cara membatasi hak akses penggunaan sesuai dengan identitas yang mereka miliki?
- Bagaimana cara membatasi akses yang berguna untuk memproteksi *resource* dan fungsi tertentu pada suatu aplikasi?

Kebutuhan keamanan yang semakin banyak menimbulkan gagasan untuk menuliskan dasar-dasar keamanan yang diterapkan oleh *Microsoft* pada *windows*, gagasan tersebut tertuang dalam skripsi ini. Penulisan skripsi ini bertujuan untuk lebih mengenalkan keamanan *Windows* kepada teman-teman dengan harapan agar hasil dari penulisan skripsi ini dapat dikembangkan.

Penyusunan skripsi ini merupakan salah satu kewajiban yang harus ditempuh oleh mahasiswa Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta untuk melengkapi persyaratan sebelum lulus Strata 1 (S1).

Atas tersusunnya Skripsi ini, tidak lupa saya sampaikan terima kasih kepada :

1. Bapak Melwin Syafrizal, S.kom, M.Eng, selaku dosen pembimbing yang telah memberikan petunjuk terhadap tata cara penulisan serta memberikan pemahaman tentang dasar keamanan.
2. Jean Seda selaku *IT Enginer* pada *Microsoft Corporation Cech* yang telah bersedia memberikan panduan dalam penelitian yang penulis lakukan.
3. Kedua orang tua yang selalu memberikan dukungan dalam segala hal selama kuliah di STMIK AMIKOM Yogyakarta.

Penulis menyadari sepenuhnya bahwa penyusunan skripsi ini masih jauh dari kesempurnaan, oleh karena itu penulis mengharapkan adanya kritik dan saran yang membangun agar penelitian ini dapat dikembangkan kembali untuk kemajuan bersama. Semoga penulisan skripsi ini dapat berguna bagi kita semua.

Yogyakarta, Mei 2010

Penulis

DAFTAR ISI

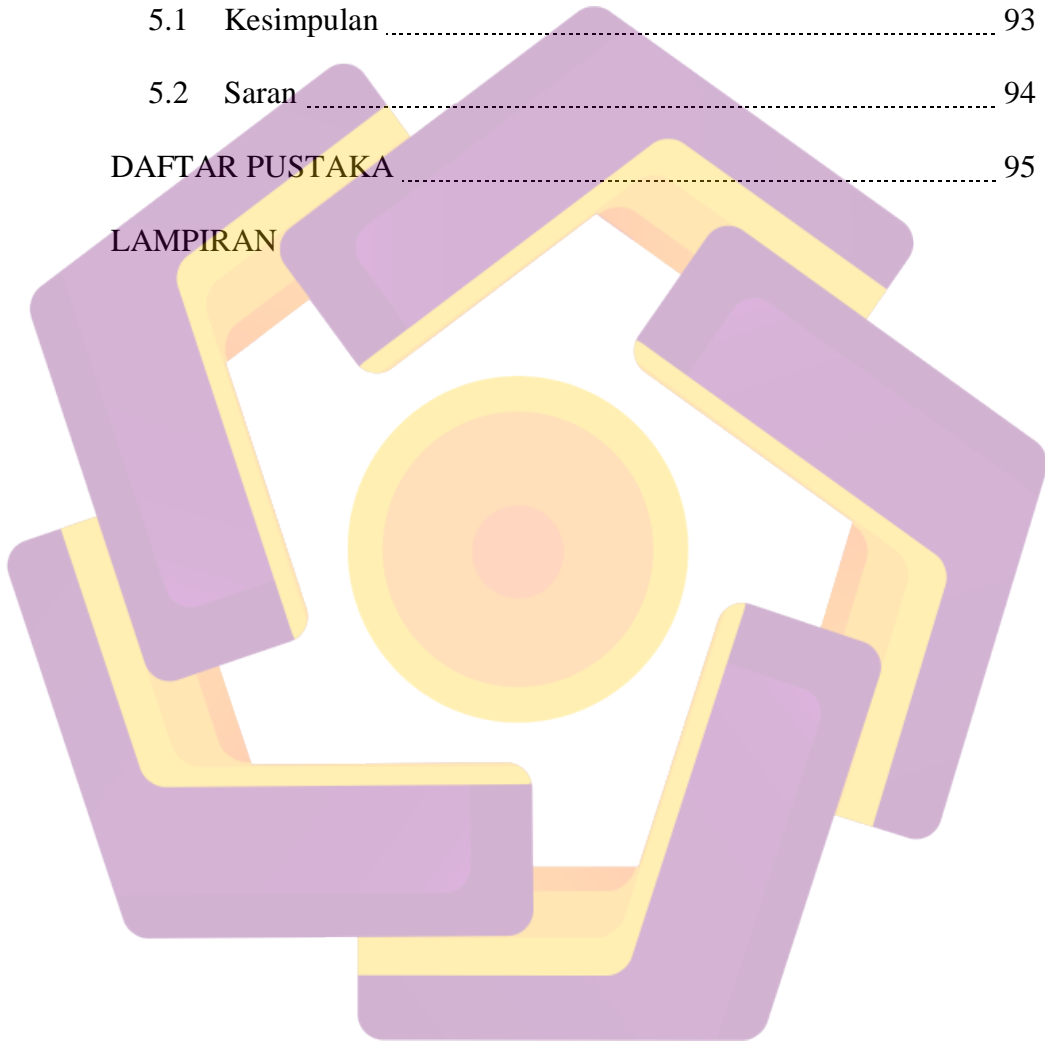
Halaman Cover	i
Halaman Judul	ii
Halaman Persetujuan	iii
Halaman Pengesahan	iv
Pernyataan Keaslian	v
Kata Pengantar	vi
Daftar Isi	viii
Daftar Tabel	xiii
Daftar Gambar	xiv
Daftar Singkatan	xvii
Intisari	xix
Abstract	xx
I. PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	4
1.6 Metode Pengumpulan Data	4
1.7 Sistematika Penulisan Laporan	5

II.	LANDASAN TEORI	6
2.1	Microsoft Windows	6
2.1.1	Windows Xp	6
2.2	Keamanan komputer	8
2.3	Windows Security	9
2.3.1	NETFramework	11
2.3.1.1	Common Language Infrastructure	13
2.3.1.2	Security	14
III.	ANALISIS DAN PERANCANGAN SYSTEM	17
3.1	Sumber Daya Security Windows	17
3.1.1	Authentication.....	17
3.1.1.1	Rencana Pembuatan Program	17
3.1.1.1.1	Flowchart	19
3.1.1.1.2	DFD	20
3.1.1.2	Rancangan Form	21
3.1.1.3	Script	21
3.1.2	Authorization	28
3.1.2.1	Rencana Pembuatan Program	28
3.1.2.2.1	Flowchart	29
3.1.2.2.2	DFD	30
3.1.2.2	Rancangan Form.....	30
3.1.2.3	Script	31
3.2	Kelemahan Security Windows	33

3.2.1	Authentication.....	33
3.2.1.1	Logon Security.....	35
3.2.1.2	Account	41
3.2.1.2.1	Administrator	41
3.2.1.2.2	Create New Account	43
3.2.2	Authorization	43
3.2.2.1	My Documents	44
3.2.2.2	Security File	45
3.3	Optimalisasi Security Windows	47
3.3.1	Authentication	47
3.4.1.1	Rancangan Program	48
3.4.1.1.1	Flowchart	49
3.4.1.1.2	Data Flow Diagram	50
3.4.1.2	Script	51
3.4	Authorization	54
3.4.1	Permission	54
3.4.2.1	Rancangan Program	55
3.4.2.1.1	Flowchart	55
3.4.2.1.2	Data Flow Diagram	56
3.4.2.2	Rancangan Form	57
3.4.2.3	Script	57
3.4.2	Cryptography	60
3.4.2.1	Rancangan Program	60

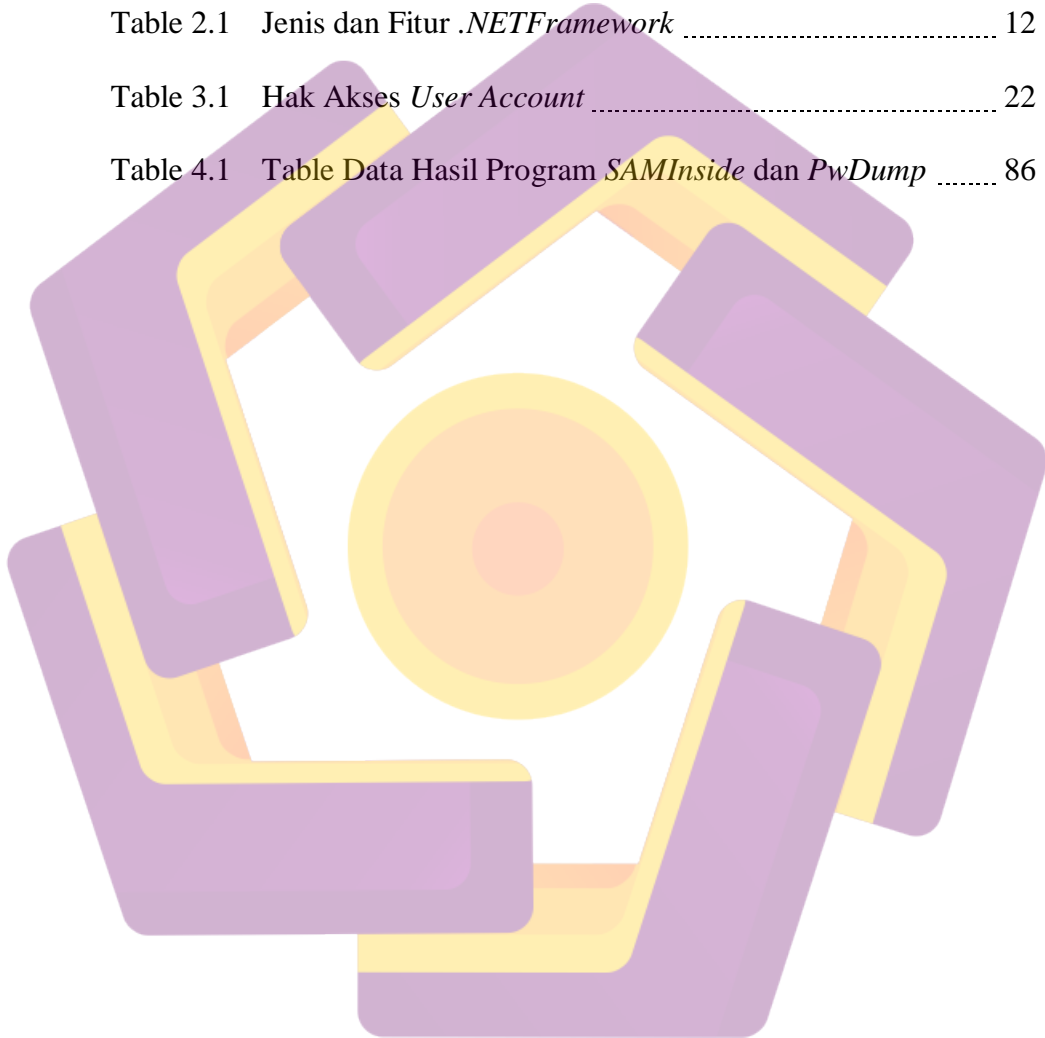
3.4.2.1.1	Flowchart	61
3.4.2.1.2	Data Flow Diagram	62
3.4.2.2	Rancangan Form	63
3.4.2.3	Script	63
IV.	IMPLEMENTASI DAN PEMBAHASAN	66
4.1	Implementasi Analisis Security Windows	66
4.1.1	Program Authentication	66
4.1.1.1	Implementasi Program	68
4.1.1.2	Pembahasan Hasil Program	69
4.1.2	Program Authorization	71
4.1.2.1	Implementasi Program	72
4.1.2.2	Pembahasan Hasil Program	73
4.1.3	Pembahasan Security Windows	76
4.2	Kelemahan Security Windows	77
4.2.1	Implementasi Program	77
4.2.2	Pembahasan Hasil Program	79
4.3	Optimalisasi Security Windows	80
4.3.1	Logon Security	80
4.3.1.1	Implementasi Program	81
4.3.1.2	Pembahasan Hasil Program	82
4.3.2	Permission	83
4.3.2.1	Implementasi Program	84
4.3.2.2	Pembahasan Hasil Program	85

4.3.3 Cryptography	87
4.3.3.1 Implementasi Program	89
4.3.3.2 Pembahasan Hasil Program	90
V. Penutup	93
5.1 Kesimpulan	93
5.2 Saran	94
DAFTAR PUSTAKA	95
LAMPIRAN	



DAFTAR TABEL

Table 2.1	Jenis dan Fitur <i>.NETFramework</i>	12
Table 3.1	Hak Akses <i>User Account</i>	22
Table 4.1	Table Data Hasil Program <i>SAMInside</i> dan <i>PwDump</i>	86

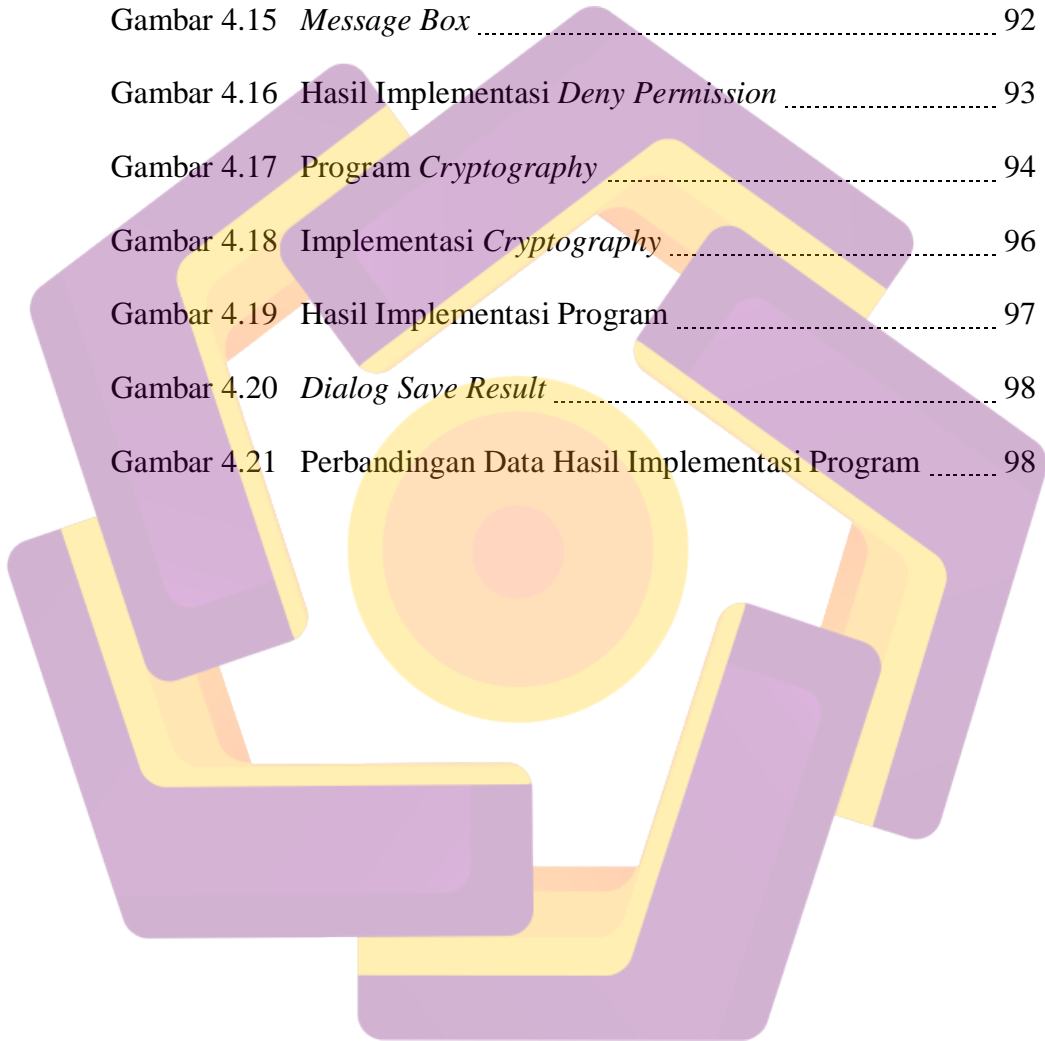


DAFTAR GAMBAR

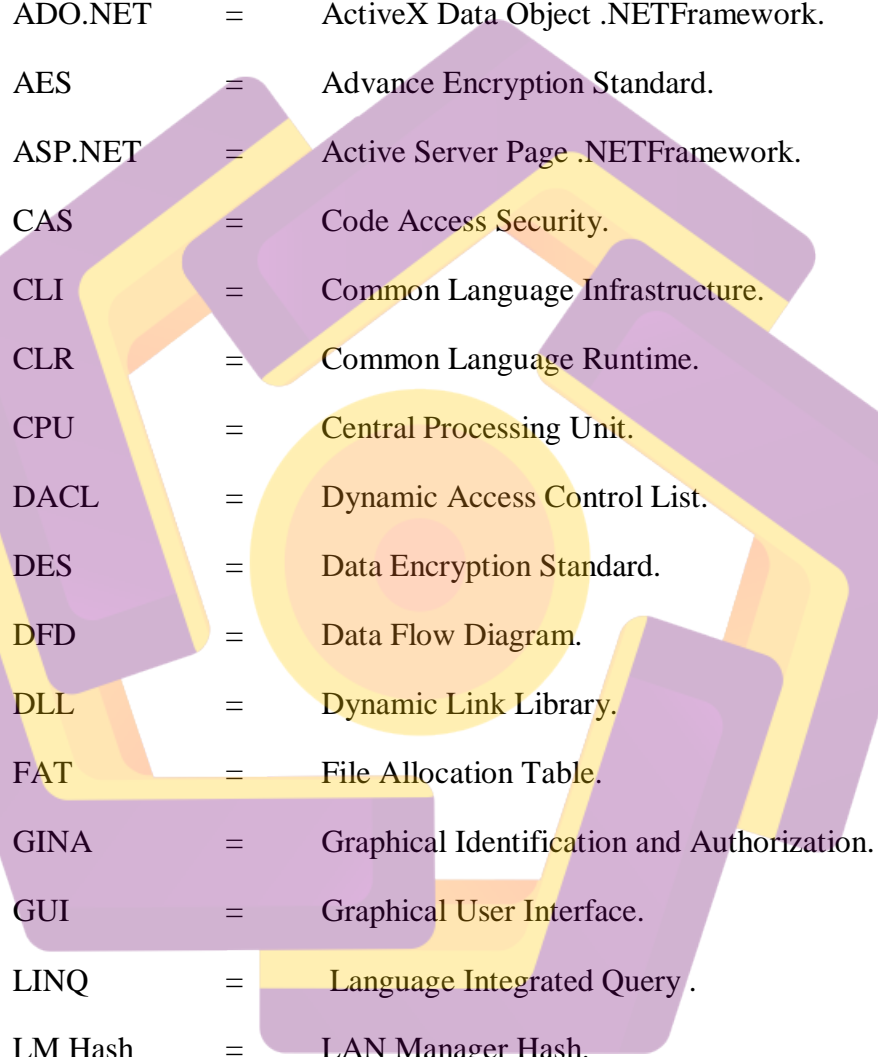
Gambar 2.1. Cara Kerja <i>Authentication</i> dan <i>Authorization</i>	11
Gambar 2.2. Hubungan antara <i>CLR</i> dan <i>CLI</i>	15
Gambar 2.3. <i>NETFramework</i>	16
Gambar 3.1. <i>Logon Screen</i>	19
Gambar 3.2. <i>Password Police</i>	20
Gambar 3.3. <i>Registry Editor</i>	27
Gambar 3.4. <i>Dialog Advance Attribute</i>	28
Gambar 3.5. Kinerja <i>Authentication</i>	29
Gambar 3.6. Proses <i>Authentication</i>	20
Gambar 3.7. <i>Flowchart Analisis Authentication</i>	32
Gambar 3.8. <i>DFD Analisis Authentication</i>	33
Gambar 3.9. Rancangan Form Analisis	34
Gambar 3.10. <i>Permission User for System</i>	41
Gambar 3.11. Proses <i>Permission</i>	42
Gambar 3.12. <i>Flowchart Analisis Permission</i>	43
Gambar 3.13. <i>DFD Analisis Permission</i>	44
Gambar 3.14. Rancangan Form Analisis <i>Permission</i>	45
Gambar 3.15. Proses <i>Cryptography</i>	47
Gambar 3.16. Proses <i>Logon Security (Continued)</i>	48
Gambar 3.17. Proses <i>Logon Security (end)</i>	49
Gambar 3.18. <i>SAM</i> dan <i>SYSTEM</i>	50

Gambar 3.19. <i>SAMInside</i>	51
Gambar 3.20. <i>System Volume Information is Denied</i>	52
Gambar 3.21. <i>Folder System Volume Information</i>	52
Gambar 3.22. <i>Flowchart Gina Stub</i>	56
Gambar 3.23. <i>DFD Gina Stub</i>	57
Gambar 3.24. <i>Flowchart Program Permission</i>	62
Gambar 3.25. <i>DFD Program Permission</i>	63
Gambar 3.26. <i>Rancangan Form Program Permission</i>	64
Gambar 3.27. <i>Flowchart Program Cryptography (Continued)</i>	67
Gambar 3.28. <i>Flowchart Program Cryptography (end)</i>	68
Gambar 3.29. <i>DFD Program Cryptography</i>	69
Gambar 3.30. <i>Rancangan Form Program Cryptography</i>	70
Gambar 3.31. <i>Ilustrasi kinerja generator Rfc2898DeriveBytes</i>	71
Gambar 4.1 <i>Program Analisis Authentication</i>	74
Gambar 4.2 <i>Implementasi Authentication</i>	75
Gambar 4.3 <i>Program Analisis Permission</i>	78
Gambar 4.4 <i>File Index.dat</i>	80
Gambar 4.5 <i>Implementasi Permission untuk Index.dat</i>	80
Gambar 4.6 <i>Message Box Error</i>	82
Gambar 4.7 <i>Flowchart Security Windows</i>	83
Gambar 4.8 <i>File SAM</i>	84
Gambar 4.9 <i>Implementasi SAMInside</i>	85
Gambar 4.10 <i>Implementasi PwDump</i>	85

Gambar 4.11 Hasil Program	88
Gambar 4.12 <i>Output Program</i>	89
Gambar 4.13 <i>Permission Program</i>	90
Gambar 4.14 <i>Browser Dialog dan Main Dialog</i>	91
Gambar 4.15 <i>Message Box</i>	92
Gambar 4.16 Hasil Implementasi <i>Deny Permission</i>	93
Gambar 4.17 Program <i>Cryptography</i>	94
Gambar 4.18 Implementasi <i>Cryptography</i>	96
Gambar 4.19 Hasil Implementasi Program	97
Gambar 4.20 <i>Dialog Save Result</i>	98
Gambar 4.21 Perbandingan Data Hasil Implementasi Program	98

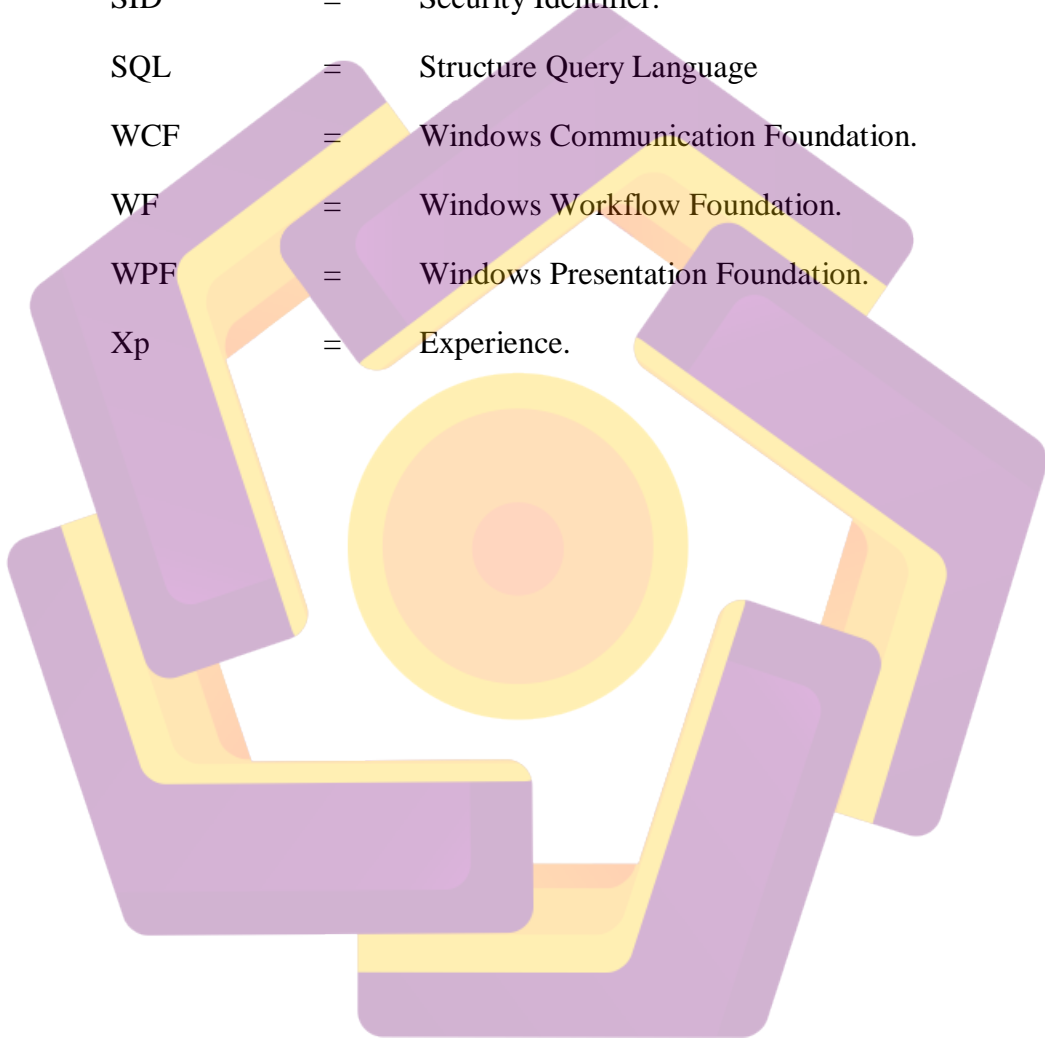


DAFTAR SINGKATAN



ACL	=	Access Control List.
ADO.NET	=	ActiveX Data Object .NETFramework.
AES	=	Advance Encryption Standard.
ASP.NET	=	Active Server Page .NETFramework.
CAS	=	Code Access Security.
CLI	=	Common Language Infrastructure.
CLR	=	Common Language Runtime.
CPU	=	Central Processing Unit.
DAACL	=	Dynamic Access Control List.
DES	=	Data Encryption Standard.
DFD	=	Data Flow Diagram.
DLL	=	Dynamic Link Library.
FAT	=	File Allocation Table.
GINA	=	Graphical Identification and Authorization.
GUI	=	Graphical User Interface.
LINQ	=	Language Integrated Query .
LM Hash	=	LAN Manager Hash.
LSA	=	Local Security Authority.
LUID	=	Locally Unique Identifier.
NT	=	New Technology.
NTFS	=	New Technology File System.
REGEDIT	=	Registry Edit.

RID	=	Relative Identifier.
SACL	=	System Access Control List.
SAM	=	Security Account Manager.
SP	=	Service Pack.
SID	=	Security Identifier.
SQL	=	Structure Query Language
WCF	=	Windows Communication Foundation.
WF	=	Windows Workflow Foundation.
WPF	=	Windows Presentation Foundation.
Xp	=	Experience.



INTISARI

Keamanan komputer adalah ilmu yang paling pesat perkembangannya karena tidak hanya untuk menunjukkan *authenticate user* tapi juga untuk menunjukkan *authorize* akses mereka. Hal yang menyebabkan kita membutuhkan keamanan adalah untuk membatasi akses penggunaan aplikasi sesuai dengan identitas yang mereka miliki. Untuk membatasi akses yang berguna untuk memproteksi *resource* dan fungsi tertentu pada suatu aplikasi. Untuk menjawab kebutuhan tersebut *windows* memberikan fitur-fitur keamanan pada sistem operasi yang dibuatnya.

Penelitian yang dilakukan diawali dengan analisis terhadap proses kerja *security* pada *windows*. Penelitian dilanjutkan dengan mencari tahu bagaimana kelemahan keamanan *windows* serta kelebihan dari fitur keamanan tersebut dan mengoptimalkan fitur tersebut untuk dapat mengamankan sumber daya *resource* pada komputer.

Kesimpulan dari hasil analisis yang telah dilakukan bertujuan untuk memberikan pengetahuan terhadap sumber daya keamanan yang ada pada *windows* serta hal yang berhubungan dengan keamanan pada *windows*, hal ini dimaksudkan untuk dapat memberikan pengetahuan kepada teman-teman yang ingin melakukan pengembangan terhadap *windows security*.

Kata-kunci: keamanan komputer, *authenticate user*, *authorize*, *windows security*

ABSTRACT

Today the growth is very rapid information technology, information technology has menjelama like clothes that we use in other words information technology has become a necessity even a lifestyle in our lives. Exchange of data is one of the trends in the world of information, sending data from one place to another. These data led to data leakage vulnerability, to reduce the leak in a security gagasanlah to avoid the leakage of data.

Security is something that most attention in the development of information science. Security is not just for show user authenticates but also to show their access Authorize. Common scenarios that cause we need more security for them to restrict access to applications in accordance with their identity. To restrict access to useful resources and to protect certain functions in an application.

Security needs of more and more led researchers to try to perform security analysis on the windows and the results are shown to give advice to my friends in order to develop a security system better.

Keywords: *Computers Security, Authenticate User, Authorize, windows security.*