Seni Teknik Hacking
Jilid 1

Ilmu hacking adalah sebuah seni yang tidak berbatas dan tidak berbentuk. Batasan dari sebuah seni hacking hanyalah kreativitas dan pengetahuan dari setiap orang.

Penulis : S'to

Seni Teknik Hacking 1
Oleh : S'to

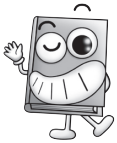
ISBN 979-98545-2-0 (jil.1)

Cetakan pertama : Desember 2004

Daftar Isi

Hack 1x01. Mencari Alamat IP Lokal 1
Hack 1x02. Mencari Alamat IP Lawan Chatting 3
Hack 1x03. Mencari Pemilik IP 8
Hack 1x04. Cara Mudah Mencari Pemilik IP 11
Hack 1x05. Mengirim Email Palsu 14
Hack 1x06. Menangkap Pengiriman Email Misterius 21
Hack 1x07. Mencari Port yang terbuka 25
Hack 1x08. Menyembunyikan Diri 28
Hack 1x09. Menangkap Penyusup 32
Hack 1x10. 100% Aman Dari Serangan Hacker : Tutup Port Anda . 35
Hack 1x11. Proteksi Terbatas : Firewall 37
Hack 1x12. Melewati Proteksi Yahoo!Groups 39
Concept : Trojan Horse 42
Hack 1x13. Trojan Horse Klasik - Optix Pro 45
Hack 1x14. Menjadi Pemburu Trojan 55
Concept 2 : Trojan di Balik LAN 64
Hack 1x15. Menggunakan Trojan di Balik LAN : Assasin 66
Hack 1x16. Trojan Horse Tanpa Instalasi Server 73
Hack 1x17. Melewati Sharing Windows 9x dan ME 78
Hack 1x18. Melewati Screen Saver Tanpa diketahui : AutoRun 84
Hack 1x19. Menjalankan Program Secara Remote 87
Hack 1x20. Disconnect Modem lawan 92
Concept : Mengatasi Proteksi Chatting Perusahaan 98
Hack 1x21. Melewati proteksi firewall dengan HTTP-Tunnel 101

Hack 1x22. Menjalankan Yahoo!Messenger dengan HTTP-Tunnel . 107
Hack 1x23. Melewati Proteksi Internet Kantor-IP 110
Hack 1x24. Melewati Proteksi Internet Kantor-Hostname 112
Hack 1x25. Melewati Proteksi Internet Kantor-MAC 114
Hack 1x26. Melewati Proteksi Internet Kantor-User Account 117
Hack 1x27. Hack 1x29. Melewati proteksi password lokal Windows NT, 2000, XP dan 2003 120
Hack 1x28. Membongkar password Office, adobe, Winzip, Paradox, Outlook, Access, IE, WordPerfect, dst 129
Hack 1x29. Melihat Password Asterix (*) 133
Hack 1x30. Membuat Windows 98 Crash secara remote 135
Hack 1x31. Mencari Bajakan Cyber 136
Hack 1x32. Melewati Proteksi Attachment Pada Email 139
Hack 1x33. Injeksi Script 141
Hack 1x34. Pemalsuan Identitas, Perampokan Nasabah 144
Hack 1x35. Google Hacking 158
Hack 1x36. Google Hacking, Carder dan Kartu Kredit 173
Hack 1x37. Google Hacking, Mendapatkan Password 177
Hack 1x38. Ancaman Gambar JPG (GDI+) 179
Index 198



Concept : Mengatasi Proteksi Chatting Perusahaan

Rossy sedang melihat ke komputernya dengan serius, tiba-tiba mukanya murung, cemberut. Tampak tangan mungilnya semakin lincah mengetik keyboardnya sehingga berbunyi klik.. klak..tut.. brakkkk !! Toongggg !! .... Woowww.... Keyboardnya telah dibanting ke kepalanya Jacky, rekan kerja yang duduk di sebelahnya. Tentu keributan segera terjadi. Jacky sebagai lelaki sejati tentu tidak terima karena bunyi kepalanya yang "Tongg", ketahuan sudah selama ini bahwa isi kepalanya kosong.

Setelah diselidiki oleh Bos, ternyata Rossy yang sibuk berchatting-ria telah diputuskan oleh pacarnya melalui ICQ. Pada saat yang bersamaan, Jacky tertawa dan tersenyum sendiri karena telah mendapatkan kepercayaan dari pacar baru dalam chattingnya. Rossy yang mengira sedang diledek oleh Jacky, akhirnya nekat melakukan tindakan bumi hangus.

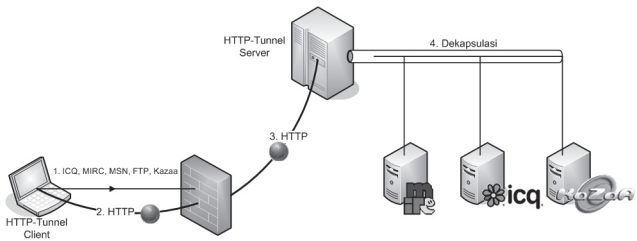
Akhirnya, Bos memberikan pengumuman sembari mengelus perutnya yang buncit "Mulai sekarang, di kantor tidak boleh chatting kecuali browsing untuk mencari informasi-informasi yang berhubungan dengan perusahaan". Kiamat sudah buat para maniak chatting.

Sudah sangat umum, di kantor-kantor yang "benar" melakukan proteksi terhadap chatting terhadap karyawannya, seperti ICQ, Mirc, Yahoo!Messenger dan gengs. Proteksi ini dilakukan seiring dengan banyaknya orang-orang seperti Rossy dan Jacky yang sangat betah di depan komputer tapi tidak satupun pekerjaan yang selesai.

Proteksi semacam ini, yang hanya memperbolehkan browsing ternyata tidak sepenuhnya bisa digunakan untuk mencegah karyawan yang pintar untuk tetap melakukan kegiatan "buaya cyber" atau kegiatan lainnya. Suatu konsep yang sangat menarik

telah diperkenalkan seiring dengan banyaknya orang-orang yang mengalami proteksi semacam ini, yaitu **HTTP Tunnel**.

HTTP Tunnel akan membungkus atau istilah mudahnya merubah format data chatting, ftp, dll ke dalam bentuk HTML. Bentuk HTML inilah yang akan mengecoh proteksi firewall. HTTP Tunnel yang terdiri atas dua bagian ini, yaitu Server dan Client sudah mulai sering digunakan seiring banyaknya proteksi yang semakin ketat.



Gambar C3-1. HTTP Tunnel

Dengan HTTP Tunnel, proteksi terhadap ICQ, MIRC, FTP, Kazaa, dll oleh firewall **(1)** bisa menjadi tidak berguna (Gambar C3-1). Dengan menggunakan HTTP Tunnel pada komputer client, paket-paket terlarang ini bisa di enkapsulasi ke dalam HTTP **(2)** sehingga bisa melewati proteksi firewall **(3)**.

Paket yang telah melewati firewall ini akan dirubah kembali oleh HTTP-Tunnel Server dan di-dekapsulasi **(4)** kembali ke bentuk aslinya seperti MIRC, ICQ, FTP, Kazaa, dll. Dengan teknik ini, proteksi chatting atau aplikasi lainnya bisa dilewati asalkan akses browsing diperbolehkan.

Anda bisa membayangkannya seperti berikut : Kwik, Kwek dan Kwak ketika dewasa menjadi penjahat yang sangat jahat sekali menggantikan posisi gerombolan si berat. Polisi memenjarakan ketiga orang ini ke Nusa kambangan di mana tidak seorangpun boleh menjenguknya.

Tentu saja Kwik, Kwek dan Kwak tidak akan bisa lagi berkomunikasi dengan paman Donald untuk merencanakan kejahatan lainnya. Tapi untunglah, sipir penjara ini dengan mudah bisa diajak bekerjasama. Untuk itulah Kwik, Kwek dan Kwak menitipkan pesan ke sipir penjara yang kemudian akan ke rumah paman Donald untuk menyampaikannya. Demikianlah, sipir penjara sebagai orang yang berhak keluar masuk lingkungan penjara telah menjadi perantara untuk Kwik, Kwek dan Kwak yang tidak mempunyai akses keluar.

Proses enkapsulasi bekerja hampir sama dengan kasus penjara ini. Penjara bagi narapidana bisa Anda bayangkan sebagai firewall untuk aplikasi IRC, ICQ, Mirc, dll. Sipir penjara adalah protokol HTTP yang tidak diblok. Uang adalah alat yang harus digunakan agar sipir penjara bersedia terus bertindak sebagai perantara dan uang ini adalah aplikasi HTTP-Tunnel ini.

Karena semua komunikasi melalui HTTP-Tunnel ini, maka server-server HTTP Tunnel yang disediakan atau yang akan digunakan ini sangat berpengaruh terhadap performance aplikasi. Artinya, jika server HTTP Tunnel ini lambat, otomatis pengguna aplikasi ini juga akan mengalami kelambatan.

Melewati proteksi firewall dengan HTTP-Tunnel

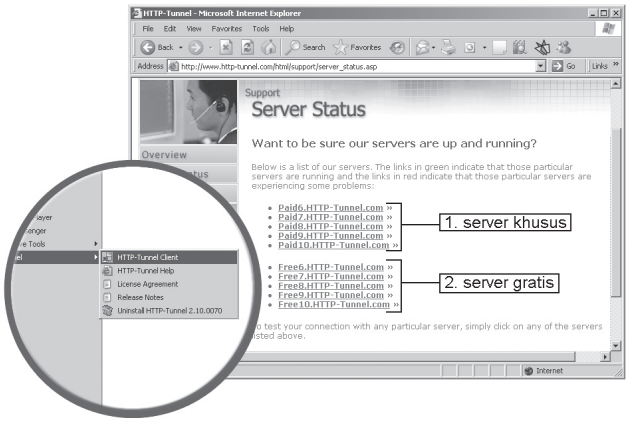
Cukup banyak aplikasi HTTP Tunnel ini di Internet dengan konsep kerja yang sama. Untuk itu, saya akan memilih salah satunya untuk dibahas di buku ini karena adanya layanan gratis walaupun dengan bandwidth yang dibatasi.

HTTP Tunnel yang saya maksudkan adalah HTTP-Tunnel yang diambil dari situs http://www.http-tunnel.com.

Terdapat 4 tahap yang akan kita lakukan untuk menggunakan HTTP-Tunnel ini, yaitu :

1. Melakukan instalasi HTTP-Tunnel Client (hanya mengklik tombol next sehingga tidak dibahas)
2. Memastikan server-server HTTP-Tunnel aktif
3. Melakukan konfigurasi HTTP-Tunnel client
4. Melakukan konfigurasi program seperti Mirc, ICQ dan Yahoo!Messenger agar melakukan koneksi melalui HTTP-Tunnel ini.

Sebelum kita memulai menjalankan program **HTTP-Tunnel Client** yang telah terinstalasi, pastikan server-server gratis yang digunakan ini dalam keadaan aktif. Untuk itu, Anda bisa mengeceknya secara online, **www.http-tunnel.com/html/support/server_status.asp** (link ini mungkin berubah) yang akan memperlihatkan dua kelompok server yaitu kelompok khusus pelanggan **(1)** dan kelompok gratis **(2)** (Gambar 21-1).

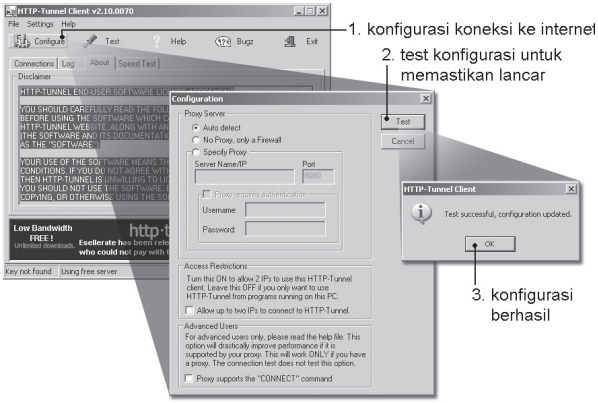


Gambar 21-1. Layanan HTTP-Tunnel

Tentu saja, server-server gratis mempunyai keterbatasan yaitu bandwidth yang disediakan sangat terbatas sedangkan server untuk pelanggan yang bayar, bandwidth yang disediakan jauh lebih besar.

Selanjutnya, HTTP-Tunnel Client yang telah terinstall harus di konfigurasi sebelum bisa digunakan. Langkah pertama konfigurasi adalah menentukan bagaimana komputer yang terinstall HTTP-Tunnel Client ini terkoneksi ke Internet.

Untuk itu, klik tombol **Configure (1)** (Gambar 21-2). Dari form **Configuration** ini, Anda bisa mengisi pilihan proxy server atau memilih **Auto Detect** agar program mencarinya sendiri. Jika Anda tidak mengetahui konfigurasi ini, tapi selama ini IE Anda berjalan lancar, nyonteklah konfigurasi dari IE melalui menu **Tools ◊ Internet Options ◊ Connections ◊ LAN Settings**.

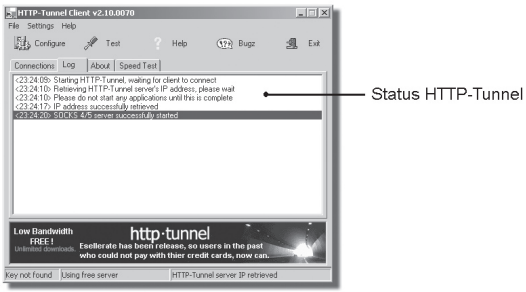


Gambar 21-2. Setting Koneksi ke Internet

Setelah pengisian **Proxy Server** selesai dilakukan, klik tombol **Test (2)**. Jika tombol Test memberikan informasi berhasil atau "**Test successful, configuration updated**" **(3)** maka HTTP-Tunnel Anda sudah siap digunakan. Mudah bukan ?

Setelah konfigurasi selesai, pada tabulasi **Log** (Gambar 21-3) Anda akan melihat status dari HTTP-Tunnel. Baris pertama menampilkan "**Starting HTTP-Tunnel, waiting for client to connect**". Baris kedua menampilkan "**Retrieving HTTP-Tunnel server's IP Address**" yang berarti HTTP-Tunnel Anda sedang mencari server HTTP-Tunnel yang aktif di Internet.

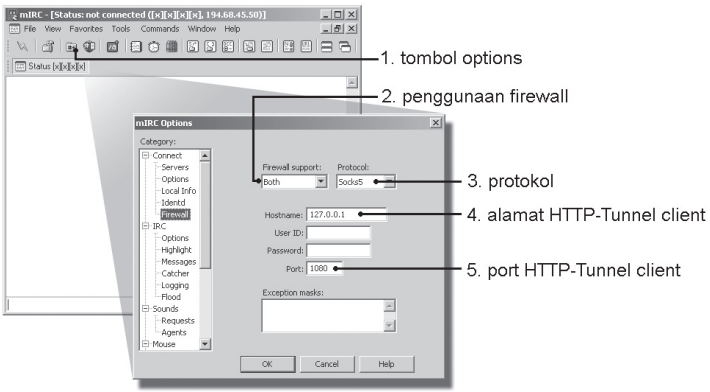
Baris ketiga menampilkan "**Please do not start any applications until this is complete**". Baris selanjutnya yang akan ditampilkan adalah "**IP Address successfully retrieved**" yang disertai dengan "**Socks 4/5 Server Started**". Kini, HTTP-Tunnel Client Anda sudah siap digunakan oleh aplikasi-aplikasi yang sebelumnya terproteksi.



Gambar 21-3. Status HTTP-Tunnel

Langkah selanjutnya adalah melakukan setting pada aplikasi client, baik itu mIRC, FTP, ICQ, dll agar memanfaatkan HTTP-Tunnel ini. Pada dasarnya Anda melakukan setting pada bagian firewall/proxy agar menunjuk ke alamat HTTP-Tunnel Client.

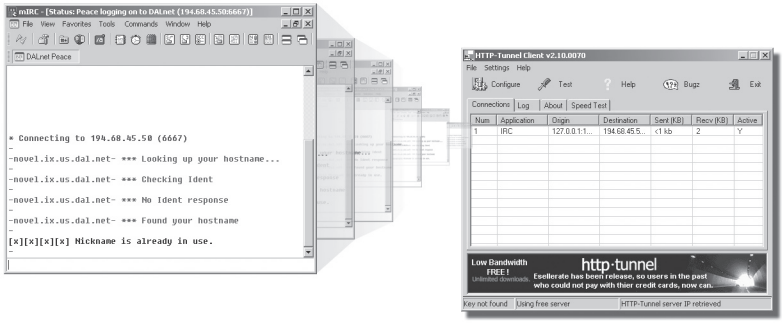
Sebagai contoh, saya akan melakukan setting di mIRC agar menggunakan program HTTP-Tunnel Client di komputer saya yang telah dijalankan dan di-konfigurasi (gambar 21-4).



Gambar 21-4. Setting mIRC agar memanfaatkan HTTP-Tunnel

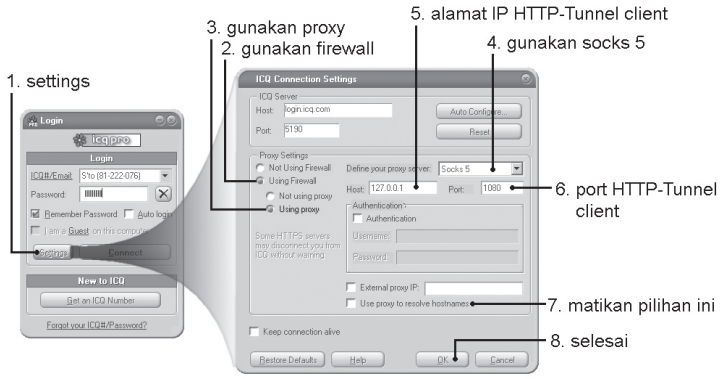
Pada program mIRC (saya menggunakan versi 6.16), klik tombol **Options (1)**, pilih kategori **Connect ⇨ Firewall**. Pada bagian **Firewall support (2)**, pilih **Both (2)** agar mIRC Anda selalu menggunakan HTTP-Tunnel sedangkan pada **Protocol (3)**, gunakan **Socks5**.

Pada kolom **Hostname (4)**, isilah alamat IP dari komputer yang menjalankan HTTP-Tunnel ini. Karena saya menjalankan HTTP-Tunnel Client dengan mIRC pada komputer yang sama, maka saya mengisikan alamat localhost, yaitu **127.0.0.1**. Port yang digunakan oleh HTTP-Tunnel adalah **1080** sehingga Anda harus mengisi bagian **Port (5)** dengan angka **1080**.



Gambar 21-5. mIRC memanfaatkan HTTP-Tunnel untuk koneksi

Setelah setting mIRC selesai dilakukan, kini chatting melalui mIRC bisa dilakukan seperti biasa. Pada saat mIRC terkoneksi ke server IRC, program HTTP-Tunnel Client segera akan menampilkan koneksi yang terjadi ini pada tabulasi **Connection** (Gambar 21-5).



Gambar 21-.6. ICQ Melalui HTTP-Tunnel

Untuk aplikasi ICQ (saya menggunakan versi 2003b), Anda bisa melakukan setting dengan mengklik tombol **Settings (1)** yang akan menampilkan konfigurasi tata cara koneksi ke Internet. Pada pilihan Proxy Settings, pilihlah pilihan **Using Firewall (2)** dan **Using proxy(3)**. Untuk **Define your proxy server (4)**, gunakan **Socks 5** sedangkan **Host (5)** diisi dengan alamat IP dari HTTP-Tunnel Client Anda.

Jika ICQ dan HTTP-Tunnel Client berada pada komputer yang sama, Anda bisa mengisi dengan alamat **127.0.0.1** yang berarti "komputer lokal". **Port (6)** yang digunakan oleh HTTP-Tunnel Client adalah **1080** jadi isilah dengan angka ini. Jangan lupa Anda harus mematikan pilihan **Use proxy to resolve hostnames (7)**.

Setelah mengklik tombol **OK (8)**, maka ICQ Anda telah siap menggunakan HTTP-Tunnel untuk melewati proteksi dari admin IT yang angkuh (atau Anda?).