Sniffing? Cain & Abel Saja!

Farhan Perdana
kuroiunagi@gmail.com
http://aniplasma.co.nr

SNIFFING ITU APA?

Sniffing, alias mengendus, adalah suatu kegiatan mengendus-endus seperti namanya. Untuk istilah bidang informatika, sniffing adalah pekerjaan menyadap paket data yang lalu-lalang di sebuah jaringan. Paket data ini bisa berisi informasi Mengenai apa saja, baik itu username, apa yang dilakukan pengguna melalui jaringan, termasuk mengidentifikasi komputer yang terinfeksi virus, sekaligus melihat apa yang membuat komputer menjadi lambat dalam jaringan. Bisa juga untuk menganalisa apa yang menyebabkan jaringan macet. Jadi bukan sekedar untuk kejahatan, karena semuanya tergantung penggunanya, tapi umumnya dilakukan karena ISENG☺.

Sniffing bisa dilakukan tidak berarti karena masalah komputer atau system operasi, tapi system dari jaringan sendirilah yang bermasalah. Misalnya pada system jaringan yang menggunakan hub, komputer-komputernya sombong oleh sebab permintaan data maupun pengiriman data disiarkan ke seluruh komputer dalam jaringan, dan hanya komputer yang butuh saja yang Mengambil data yang ditujukan padanya sedangkan komputer lain akan mengacuhkannya. Tetapi semua itu akan lain jika salah satu komputer tersebut menggunakan sniffer atau pengendus. Semua data yang disiarkan termasuk ke komputer tersebut akan ditangkap, terlepas dari data tersebut adalah permintaan dari komputer tersebut atau tidak. Anda yang pernah membaca buku *Animorphs* karangan *K.A. Applegate* tentu mengetahui cara bicara Visser Three. Visser Three yang menggunakan bahasa pikiran yang seharusnya bisa ditujukan ke orang-orang tertentu karena kepongahannya selalu menyiarkan bahasa pikirannya tanpa dibatasi. Begitulah sifat-sifat jaringan yang menggunakan hub.

Sniffing juga termasuk mengendus data-data yang disembunyikan dalam komputer, termasuk yang dienkripsi karena memang inti dari sniffing sama seperti anjing pelacak di bandara Soekarno-Hatta yang memburu Bandar Narkoba.

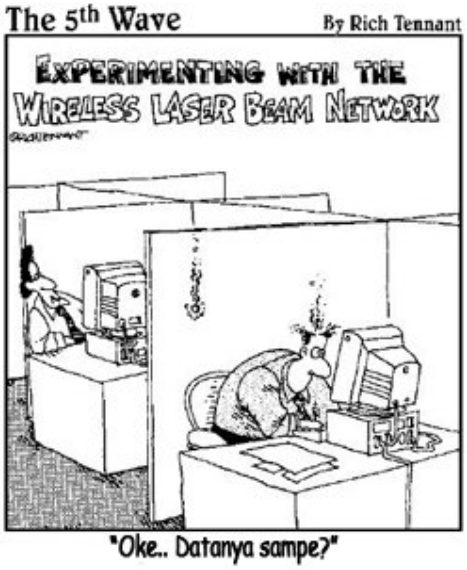
Melakukan sniffing bukan berarti anda sama dengan anjing. Tidak! Anda dan anjing memiliki banyak Perbedaan baik dari segi fisik maupun mental. Seseorang tidak bisa menyamakan anda dengan anjing. Tentu saja anda lebih baik dari Anjing (atau sebaliknya? Hanya anda dan tuhan yang tahu). Bukankah semuanya tergantung dari niat? Untuk masalah niat, anda bisa menghubungi Bang Napi.

Yang perlu anda ingat dalam melakukan Sniffing, adalah perbedaan antara Sniffing yang professional dan Sniffing asal-asalan. Sniffing memang Sniffing, tapi Sniffing yang professional adalah jika anda bisa menganalisa hasil Sniffing anda sendiri, merangakai informasi yang anda dapatkan dari hasil Sniffing menjadi suatu kesimpulan. Kira-kira sama seperti detektif yang membuat hipotesa dari bukti-bukti yang ada, alibi, serta keterangan saksi-saksi. Bukan hanya sekedar mencari password yang berkeliaran.

Anda mungkin pernah mendengar lelucon seperti ini :
"Seorang lelaki masuk ke sebuah bar dan berbicara dengan Andi. Andi kemudian berkenalan dengan lelaki tersebut. Ternyata lelaki tersebut bernama Herman. Andi bertanya kepada Herman, "Apakah pekerjaan anda?"
Herman : "Saya adalah seorang pemikir logis."
Andi : "Pekerjaan seperti apakah itu?"
Herman : "Wah, susah dijelaskan, tapi kalo diberi contoh mungkin anda bisa mengerti. Coba saya tanyakan anda satu hal. Apakah anda punya kucing?"
Andi : "Ya! Betul! Dirumah saya memiliki seekor kucing!"
Herman : "Kalau begitu anda tentunya adalah penyayang binatang?"
Andi : "Ya! Betul! Dirumah saya juga memiliki 2 ekor ikan mas dan seekor parkit!"
Herman : "Kalau begitu tentunya anda senang dengan anak-anak?"
Andi : "Ya! Betul! Saya sendiri memiliki seorang anak dan mengangkat anak juga!"
Herman : "Kalau begitu tentunya anda memiliki seorang istri, betul?"
Andi : "Ya! Betul! Saya memiliki seorang istri dirumah!
Herman : "Kalau begitu tentunya anda bukanlah seorang yang Impoten, betul?"
Andi : "Betul! Saya memang tidak impotent!"
Herman : "Itulah yang disebut pemikir logis!"

Esoknya di kantor, Andi menceritakan pengalaman tersebut kepada temannya. "Tadi malam saya bertemu dengan seorang pria yang luar biasa! Pekerjaannya adalah pemikir logis." "Wah? Saya baru dengar. Apa sih pemikir logis itu?" tanya temannya. "Wah, susah dijelaskan," jawab Andi. "Tapi akan lebih mudah dengan contoh. Begini, apa kamu punya kucing dirumah?". "Tidak." Jawab temannya. "Kalau begitu kamu Impoten!".

Sekarang terserah anda, apakah anda bisa melakukan Sniffing professional seperi Herman, sang pemikir logis, atau asal-asalan seperti Andi…



CAIN & ABEL

Cain & Abel adalah sebuah program Recovery Password sekaligus Pengendus Jaringan dari Massimiliano Montoro yang bisa didownload pada http://www.oxid.it/. Jika anda belum mengetahui apa itu pengendus jaringan, mungkin kata *network analyzer* bisa membantu. Atau jika tidak, mungkin anda pernah mendengar sebuah tool bernama *ethereal* (Sekarang namanya *wireshark*-hiu kabel-)? Singkatnya, dua-duanya adalah Sniffer.

Cain & Abel mudah digunakan untuk pemula karena lebih enak dilihat untuk mata pemula :P. Lebih sedikit berwarna-warni jika dibandingkan dengan ethereal. Oke, cukup bicara tentang *ethereal* karena judul diatas berbicara mengenai Cain & Abel. Dua anak nabi Adam yang kali ini tidak saling membunuh tapi malah bekerjasama membantu anda :D.

Untuk mendapatkan Cain & Abel sangat mudah. Download saja file nya dari situs oxid, kemudian saat menginstall, hantam saja next. Tidak perlu dilihat yang lain, seperti saat anda menginstall Windows XP :P. Saya bahkan pernah mencoba untuk menggunakan Cain & Abel hasil kopi paste dari folder *Program Files* komputer teman saya dan jalannya sah-sah saja. Yang perlu diperhatikan adalah program Cain & Abel itu terdiri dari dua buah program yang terpisah. Cain, sang kakak, adalah program dengan tampilan pengendus yang sebenarnya dan memang langsung dipasang saat anda selesai menghantam next, dimana Abel, si adik, adalah remote console pada mesin target, dan tidak langsung diinstal saat anda menghantam next pada penginstalan Cain. Untuk menggunakan sang adik, ada dua cara yaitu :

Pasang pada komputer secara langsung :

1. Buka tempat cain di install, anda akan melihat abel.exe dan abel.dll. Blok keduanya kemudian klik kanan dan copy.
2. Paste keduanya di direktori WINNT
3. Jalankan abel, atau klik start-run-abel.
4. Biarkan keduanya ngobrol lewat Service Manager milik Cain (kira-kira sama kayak sms :D)
5. Untuk menguninstall, jalankan run, dan ketikkan abel –r.

Melalui remote

1. Pilih komputer yang di remote dengan menggunakan cain pada Network Tab, kemudian klik kanan icon komputer tersebut
2. Buktikan ke-adminan anda pada komputer yang di remote. Sama sepeti membuktikan diri anda ke calon mertua, apakah anda sesuai untuk si yayang :P
3. Pilih services, terus Install Abel

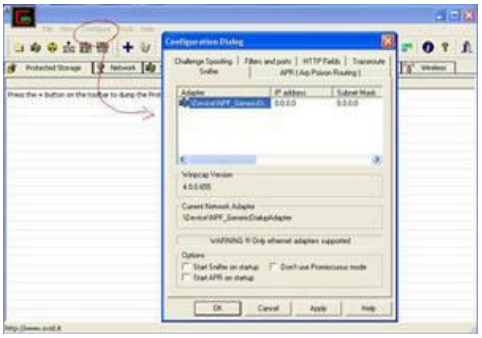
Yang menyenangkan dari program ini, adalah jika bos anda tiba-tiba muncul untuk mengecek apa yang anda lakukan dengan komputer kantor (jelas saja bos anda tidak suka ada yang menggunakan milik kantor untuk keperluan lain…), anda bisa dengan segera melarikan Cain ke System Tray dengan kombinasi tombol *ctrl+pagedown*. Nah, jika bos anda memiliki mata jeli dalam melihat System Tray (kemungkinan karena anda sering menipunya :P), anda bisa menghilangkan Cain dari layer monitor tanpa menggangu apa yang sedang Cain kerjakan dengan *Alt+Del*. Untuk mengembalikannya, cukup dengan kombinasi *ctrl+pageup*. Satu lagi, jika memang bos anda benar-benar serius, dengan satu tombol anda bisa menghilangkan semuanya dari layer, yaitu dengan menekan tombol **restart** pada CPU :P.

Fitur-Fitur Cain

❖ **SNIFFING**

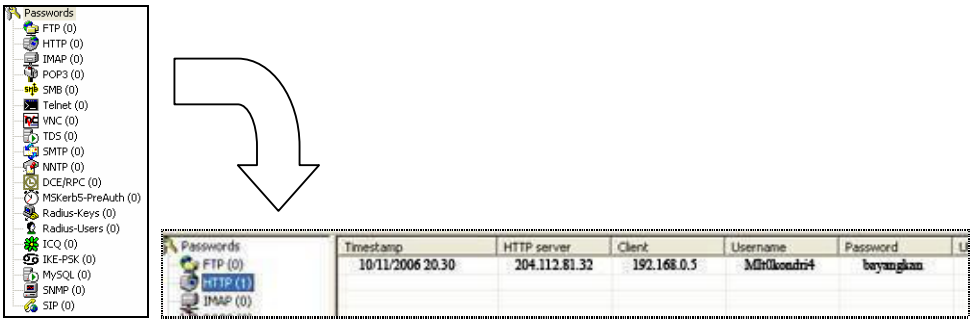
Ya! Tentu saja sniffing? Tidak masuk akal jika sebuah program sniffer fitur utamanya adalah mengedit grafik bukan? Untuk memulai melakukan sniffing sangat mudah. Pilih tab "**Sniffer**" kemudian klik icon **Start/Stop Sniffer** (nomor dua dari kiri pada bagian atas).

Jika anda menggunakan kartu jaringan lebih dari satu, jangan lupa dikonfigurasikan Cain tersebut lebih dulu untuk menggunakan kartu yang mana. Cukup dengan klik **Configure**, kemudian pada tab Sniffer, pilih kartu yang anda gunakan kemudian klik OK.



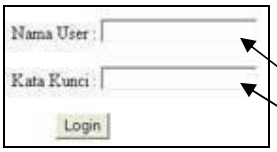
Jika proses sniffing sudah berjalan, anda bisa melihat hasilnya dengan mengklik pada sub-tab Password :

Kemudian memilih password dari aplikasi apa yang ingin anda lihat melalui list box pada bagian kiri dan semua daftar password beserta usernamenya akan tampak pada kolom di sebelah kanan:



Cain bahkan bisa merekam pembicaraan melalui Voip dan mendecodenya kemudian menyimpannya dalam format WAV!

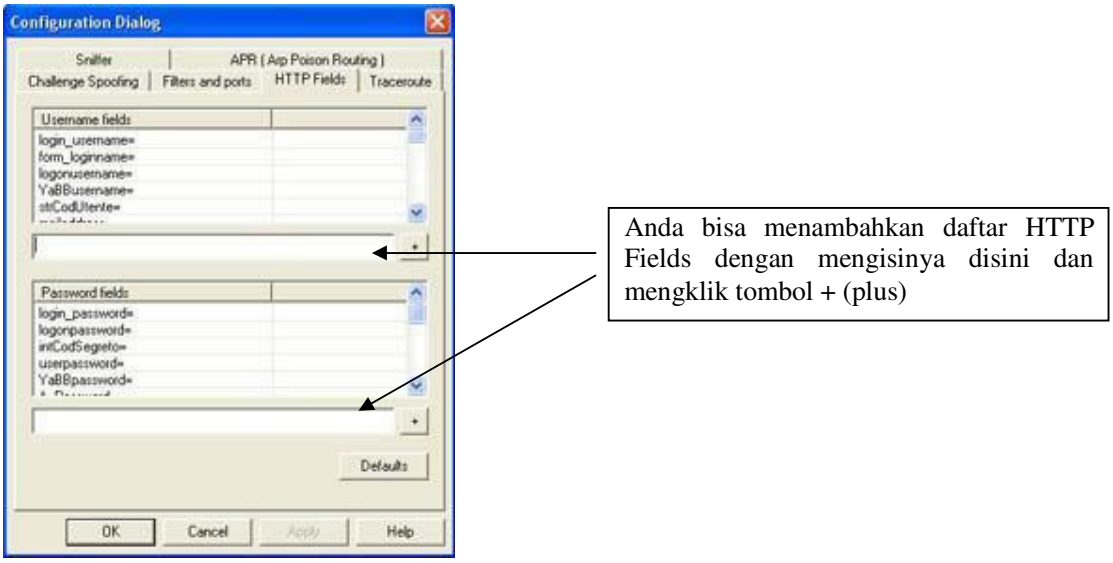
Jika dibandingkan dengan tampilan log sniffing ethereal dimana kita harus mencari-cari passwordnya, Cain memang lebih enak karena passwordnya sudah dipilah-pilah. Hal ini bisa ada, karena cain memiliki apa yang bernama HTTP Fields Tab, yaitu kumpulan dari nama-nama text box yang mungkin digunakan. Jelasnya begini. Jika anda pernah melihat sebuah login form seperti ini :



Nah, login form seperti ini biasanya memiliki kode html berupa :
* Nama User : <input type="text" name="username" size="20"> *
* Kata Kunci : <input type="text" name="password" size="20"> *

Disana bisa dilihat bahwa kode textbox untuk *Nama User* adalah **username** dan kode textbox untuk *Kata Kunci* adalah *password*. Nah, Cain menggunakan sebuah daftar panjang dari kemungkinan nama-nama textbox berisi username dan password tersebut, kemudian bekerja dengan mencari kata apa yang dimasukkan pada textbox yang dicurigai sebagai textbox berisi username dan password.

Daftar nama textbox Cain ini sendiri dapat dilihat dan diubah melalui **Configure**, pada tab **HTTP Fields**. Jika sekiranya anda menemukan sebuah situs yang nama textboxnya tidak terdapat pada daftar HTTP Fields Cain, anda bisa menambahkannya sendiri.



Jadi cara kerja pada Cain adalah menyaring isi dari log yang berhasil diendus dengan menyaring kata yang terdapat pada textbox login sebuah situs yang disesuaikan dengan daftar HTTP Fields.

Untuk program semacam ICQ tidak perlu ditambahkan, karena ICQ adalah sebuah program, bukan sebuah situs yang melalui protokol HTTP. Jika suatu saat ICQ mengganti nama textbook username dan passwordnya, yang perlu anda lakukan hanyalah mengganti Cain dengan versi yang lebih baru.

- **Pembuat** : Buat nama textbox anda seunik mungkin. Misalnya *" katakuncibukandisini"*
- **Pengendus** : Buka situs si **pembuat** dan lihat sourcenya, kemudian ambil nama textboxnya.
- **Pembuat** : Beli nama domain di www.co.nr atau gunakan saja versi gratisnya sehingga saat **pengendus** membuka situs anda dan mau ngeliat source codenya, isinya hanyalah keyword dari www.co.nr
- **Pengendus** : Buka situs **pembuat** dan lihat linknya untuk mengetahui lokasi asli dari domain pembuat, akses filenya melalui domain asli, kemudian lihat kodenya.
- **Pembuat** : Ganti semua URL pada link di situs dengan penunjukan absolut melalui domain dari www.co.nr agar domain asli tidak diketahui.
- **Pengendus** : Lihat informasi mengenai lokasi dari domain asli melalui properties pada Gambar yang terdapat pada situs **pembuat**.
- **Pembuat** : Ganti semua URL lokasi gambar di situs dengan penunjukan absolut melalui domain dari www.co.nr agar domain gambar asli tidak diketahui.
- **Pengendus** : Gunakan koneksi yang amat sangat lambat dan buka situs **pembuat**. Saat pengalihan dari Domain co.nr ke domain asli, nama domain asli akan terlihat pada ujung kiri bawah status bar browser, misalnya *(opening http://www.freewebs.com/joni...)*
- **Pembuat** : Buang servis dari www.co.nr dan gunakan Cold Fusion.
- **Pengendus** : Sandera *istri/pacar* si **pembuat** dan terror dia agar memberitahu nama textbox.
- **Pembuat** : Telepon polisi dan tetap gunakan Cold Fusion.
- **Pengendus** : Gunakan saja ethereal, dan lihat log hasil sniffing secara teliti untuk menemukan password.

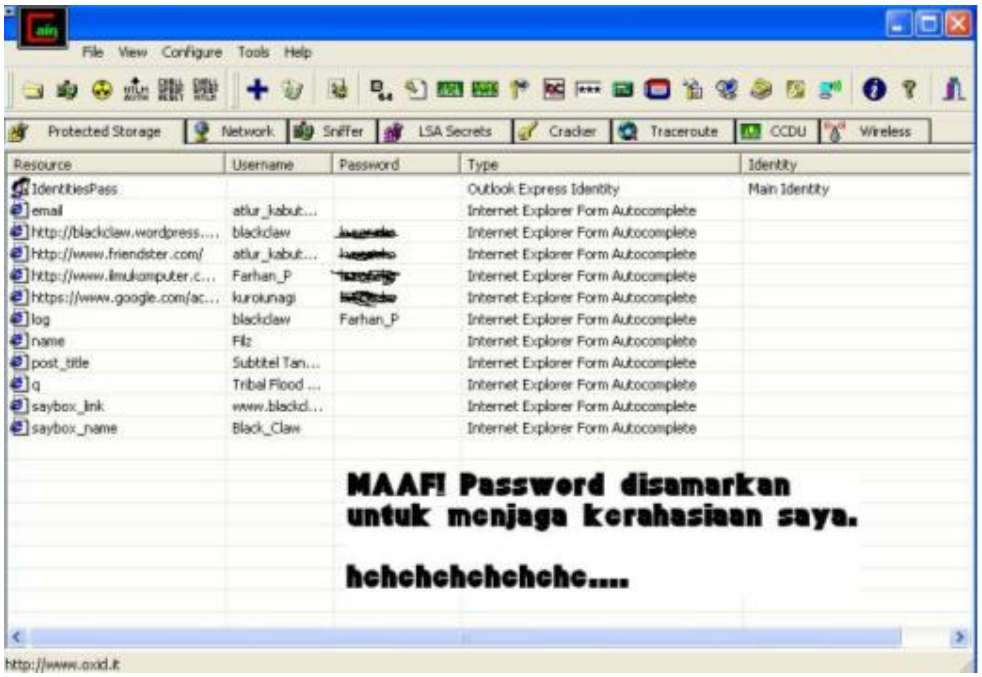
❖ **Protected Storage Password Manager**

Anda bisa melihat password-password dari program-program semacam Outlook, Outlook Express, Outlook Express Identities, Outlook 2002, Internet Explorer atau MSN Explorer yang ada pada komputer yang dipasangi Cain. Caranya, jalankan Cain, kemudian pilih tab *protected storage* (catatan : tab ini adalah tab default saat anda menjalankan cain) kemudian anda klik tanda + (plus) yang memiliki screen tip "add to list" berwarna biru dibagian atas sebelah kanan lambang tong sampah. Anda juga bisa dengan cepat melakukannya dengan menggunakan tombol insert pada keybord.

Mengapa ini bisa terjadi? Begini. Sistem penyimpanan password pada windows memang memiliki system enkripsi data bernama MicrosoftCryptoApi, yang disesuaikan dengan password serta username pada windows logon, untuk membatasi penggunaan password pada komputer yang memiliki lebih dari satu user.

Hal ini bisa ditemukan pada :
HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider\.
Nah, kebetulan (atau mungkin bukan kebetulan?) Cain memiliki decodernya

Yang tersimpan antara lain :
- *Password MS Outlook 2002 (POP3, SMTP, IMAP, HTTP)*
- *Password Outlook Express (POP3, NNTP, SMTP, IMAP, HTTP, LDAP, HTTP-Mail)*
- *Password Outlook Express Identities*
- *Password MS Outlook (POP3, NNTP, SMTP, IMAP, LDAP, HTTP-Mail)*
- *Password Sign In MSN Explorer*
- *Auto Complete MSN Explorer*
- *Password protected sites Internet Explorer*
- *Auto complete Internet Explorer*



Cain membukanya : Tidakkah setelah melihat ini anda berpikir untuk beralih ke IGOS?

❖ Credential Manager Password Decoder

Atau dikenal dengan bahasa begonya yaitu : Pembaca Password Jaringan (Network Password) pada windowsXP/2003. Password tersebut tentu saja menggunakan enkripsi, tapi *Todd Sabin*, melalui programnya yang terkenal yaitu ***PWDUMP2***, menemukan cara untuk melepas proteksinya melalui *dll Injection.* Mudahnya begini. Saat anda memberikan password dan memutuskan komputer untuk mengingatnya supaya anda tidak perlu capek menulisnya lagi, komputer akan menyimpannya pada

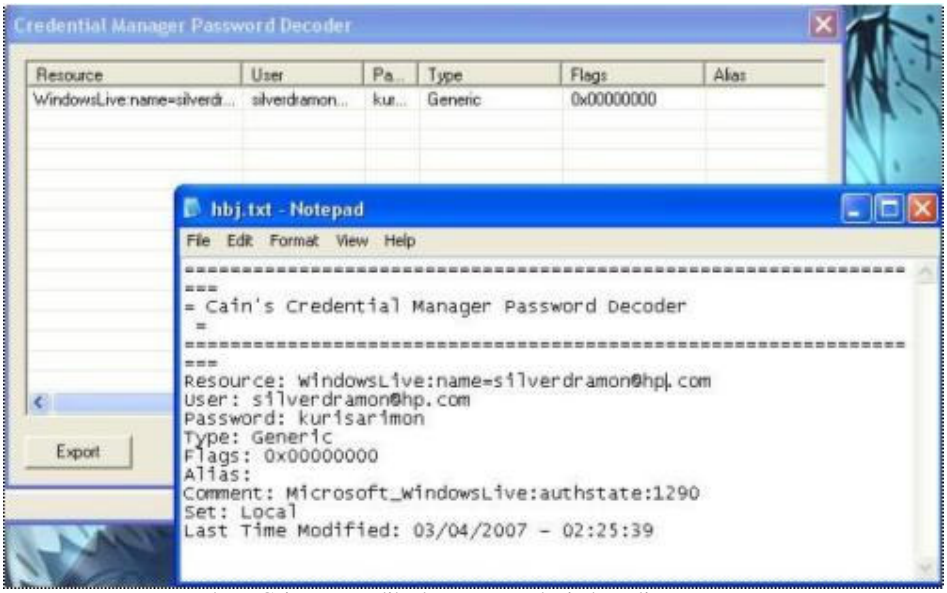
"Documents and Settings->Username->Application->Data->Microsoft->Credentials-> Username ->Credentials"

atau pada :

"Documents and Settings->Username->Local Settings->Application->Data->Microsoft->Credentials-> Username -> Credentials".

Memang ada beberapa data yang bisa dilihat dengan mata telanjang. Tapi beberapa yang penting, akan dikunci oleh enkripsi kepala keamanan komputer anda.

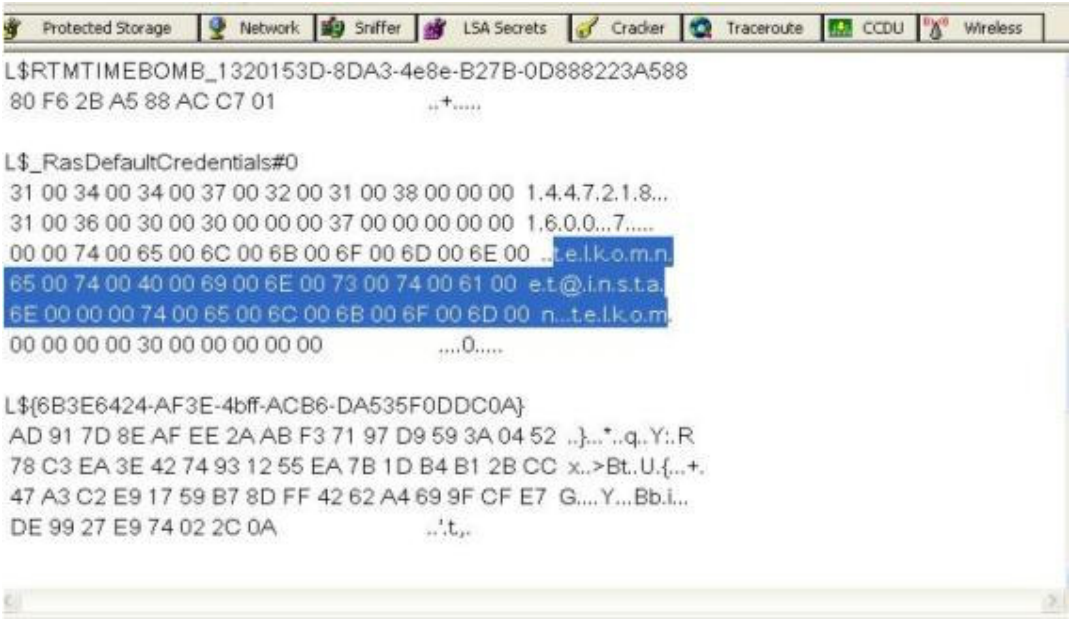
Nah, kalau sudah begini, Program akan mengirim pesan yang sudah disamakan validitas keamanannya dengan LSASS (Local Security Authority Subsystem Process-Satpamnya komputer), dengan menyamar sebagai satpam, ia akan menggunakan fungsi DumpCF dari abel untuk meminta lsarv.dll pada c:\windows\system32 untuk memberikan LsaICryptUnprotectData, kemudian menerjemahkannya. Bingung? Saya juga bingung untuk menjelaskan. Jika anda bingung, anda bisa membaca mengenai cara kerja penyimpan password jaringan ini pada : http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/dpapiusercredentials.asp
Untuk menggunakannya pada program cain, klik **tools->Credential Password Manager Decoder**, atau klik iconnya yang berlambang **mata biru dan kunci kuning** di sebelah icon dengan tulisan VPN berlatar belakan hijau. Setelah anda klik, akan tampak data-data yang dienkripsi tersebut. Anda bisa juga men-savenya dalam format .txt.



gambar : Cain memperlihatkan password windows live messenger

❖ **LSA Secrets Dumper**

Digunakan untuk mendapatkan password-password yang biasanya terkandung dalam LSA. Password-password yang biasanya didapatkan dari sini adalah password dari program-program yang bukan dari local system. Anda mungkin akan sedikit bingung melihatnya. Masalahnya, cain tidak akan memberikan : "INI PASSWORDNYA!" tetapi lebih dengan menuangkan isi dari LSA untuk anda cari sendiri. Kira-kira seperti mengais-ngais dari tong sampah. Siapa tahu ada orang yang ga sengaja ngebuang kalung berlian :P.



Gambar : Informasi mengenai Login telkomnet@instan dengan Password telkom

Untuk menjalankannya, klik tab "**LSA Secrets Dumper**" klik tanda **+** (plus) yang memiliki screen tip "add to list" berwarna biru dibagian atas sebelah kanan lambang tong sampah. Anda juga bisa dengan cepat melakukannya dengan menggunakan tombol **insert** pada keyboard.

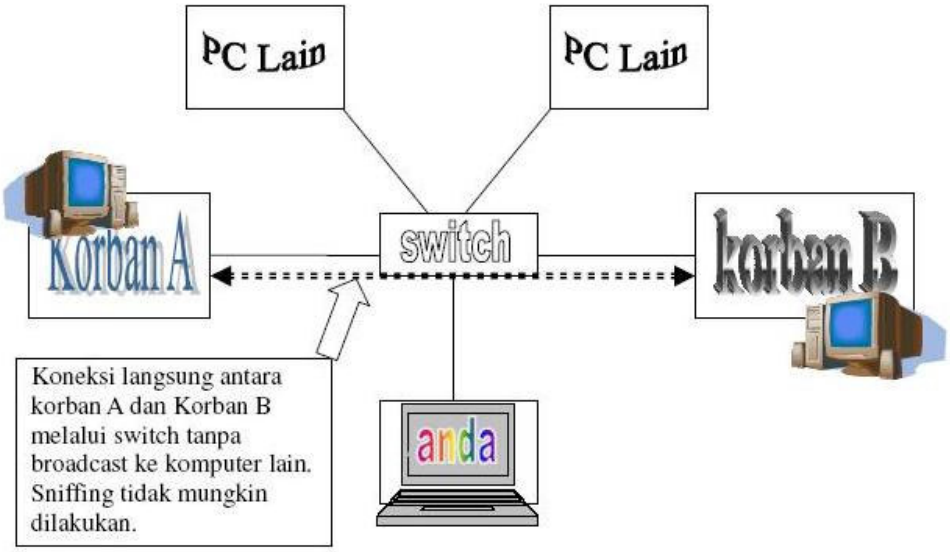
❖ **Dialup Password Decoder**

Oke, kalo ini sepertinya tidak terlalu berguna untuk warga Indonesia, Masalahnya, semua juga sudah tahu kalo untuk dial-up di Indonesia kebanyakan menggunakan Telkomnet Instan. Semua juga sudah barang tentu tahu jingle iklan
"kosong-delapan-kosong-sembilan-delapan-sembilan-empat-kaaaaa-liiiii…Telkomnet Instaaaaan…!
dengan username telkomnet@instan dan password telkom. Program seperti Revelation dari Sneadboy (http://www.snadboy.com/) juga bisa digunakan untuk melihat password semacam ini yang memang hanya disembunyikan dengan tanda * (bintang), tapi jika anda memang tahu bahwa dikomputer tersebut ada yang menggunakan dial-up selain telkomnet instant sekaligus anda tidak punya programnya Sneadboy, klik **tools** dan pilih **Dialup Password Decoder** atau klik **icon telepon berwarna kuning**.

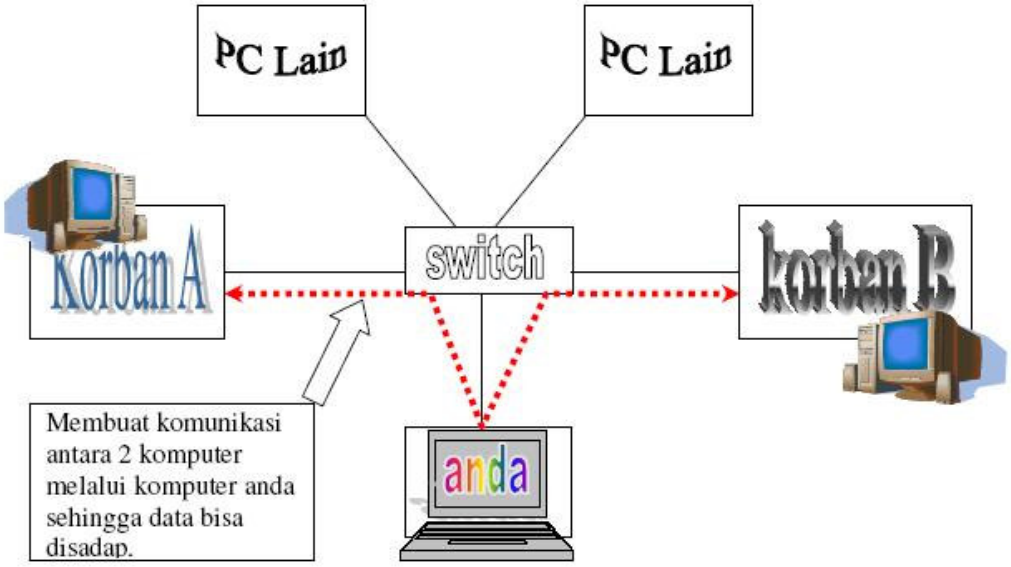
❖ **APR (ARP Poison Routing)**

Bagi anda yang bekerja jauh dari kampung halaman, misalnya anda bekerja di Jakarta dan kampung halaman anda di Brebes, dapat dipastikan setiap hari raya lebaran anda sering menjadi korban ARP Poison Routing, terutama karena anda tidak pesan tiket jauh-jauh hari sebelumnya. Ya! Itulah Calo! Si jago Man-in-the-Middle attacks. Bagaimana calo melakukannya? Pertama-tama dia akan meracuni penjual karcis bahwa dia adalah calon penumpang, kemudian ngutang karcis. Setelah itu dia akan meracuni anda dengan kata-kata bahwa dia adalah asisten penjual karcis. Kemudian, dia akan memberikan harga diatas harga karcis, bahkan sampai 10x lipat. Lalu, kelipatan 9nya akan masuk ke kantong si calo, dan dengan hati gembira dia akan memberikan harga karcis sesuai harga karcis asli ke penjual karcis asli.

Begitupun kerja APR pada Man In The Middle attack yang terinspirasi dari tehnik calo. Karena kelemahan sistem Hub dimana data disiarkan ke seluruh jaringan dan dapat ditangkap oleh komputer manapun dalam jaringan, diciptakanlah alat yang bernama *Switch*. Seperti namanya, switch memiliki kemampuan untuk menghubungkan komputer yang butuh sesuatu hanya dengan komputer yang membutuhkan sesuatu. Artinya, koneksi data antar komputer pada sistem yang menggunakan switch (atau nama kerennya Ethernet) hanya terjadi pada dua komputer sedangkan komputer yang lain pada jaringan tidak bisa mengetahui bisik-bisik mereka berdua. Nah, jika sudah seperti ini, bagaimana anda sebagai komputer ketiga bisa ikut serta mengendus isi pembicaraan mereka sedangkan syarat utama untuk melakukan sniffing adalah datanya melewati komputer anda?



Yang perlu anda lakukan adalah membuat komputer Korban A dan Korban B melakukan komunikasi melalui komputer anda, sama seperti halnya calo. Nah, saat komunikasi melewati komputer anda, otomatis data dan pembicaraan antara mereka berdua akan melalui anda sehingga bisa ditangkap oleh sniffer.



Pada Cain, fitur ARP Poison Routing adalah salah satu fitur utamanya. Untuk mengetahui bagaimana hal ini dapat terjadi, anda harus mengetahui bagaimana switch bekerja. Pada jaringan seperti ini, yang digunakan adalah alamat yang disebut alamat MAC.

Nah, jika komputer A (Korban A) ingin berkomunikasi dengan komputer B (Korban B), maka komputer A akan menyiarkan ke seluruh komputer yang ada di jaringan : *"Saya adalah komputer A dengan alamat IP *sekian* ingin berkomunikasi dengan komputer B yang IP-nya *sekian*! Berapakah alamat MAC anda komputer B?"*

Jika komputer B mendengar hal ini, maka dia akan kembali menyiarkan pada jaringan : *"Saya adalah komputer B dengan IP *sekian* dan alamat MAC saya adalah *sekian*! Hubungkan saya dengan komputer A!"*

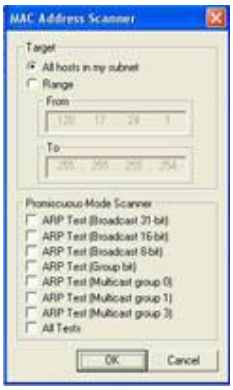
Switch yang mendengar hal ini kemudian memutuskan penyiaran pada jaringan dan hanya membatasi lalu-lintas data pada komputer A (Korban A) dan B (Korban B) saja berdasarkan alamat MAC mereka. Komputer lain pada jaringan tidak akan bisa mengetahui apa yang dibicarakan antara 2 komputer tersebut.

Nah, yang anda perlu lakukan sebagai Calo adalah saat penyiaran 2x tersebut, yaitu mengatakan ke komputer A bahwa anda adalah komputer B dan mengatakan ke komputer B bahwa anda adalah komputer A, sehingga data yang dikirimkan dari komputer A untuk komputer B diterima oleh anda. Begitupula dengan data yang dikirimkan oleh komputer B untuk komputer A diterima oleh anda. Bagaimana hal ini bisa dilakukan? Dengan mengatakan Alamat MAC komputer B kepada komputer A, dan sebaliknya, mengatakan alamat MAC komputer A kepada komputer B!

Karena anda mengatakan demikian, komputer A akan mempercayai bahwa anda adalah komputer B dan komputer B akan percaya bahwa anda adalah komputer A.

Sampai disini, data yang bisa ditangkap belum ada yang penting karena komputer A dan B masih belum bisa berkomunikasi. Untuk itu, komputer anda harus bisa meneruskan data dari komputer A ke komputer B. Untuk itu, program Cain telah menyediakan alat siap pakai. Yang

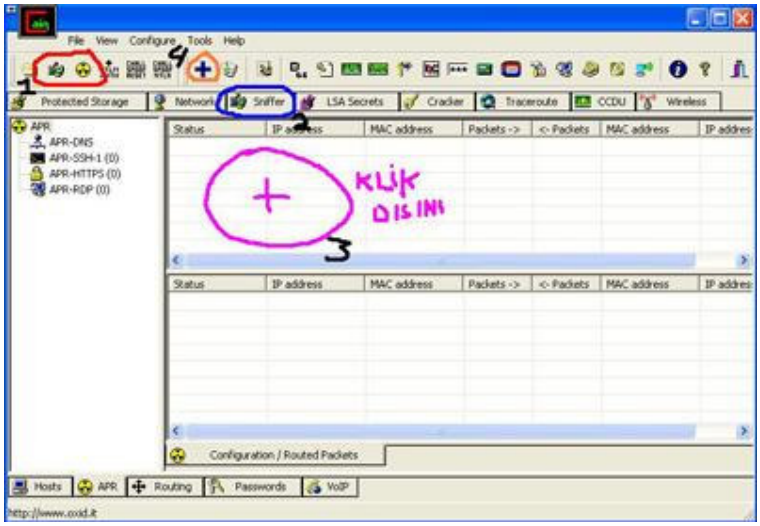
perlu anda ketahui adalah alamat Mac dari 2 komputer yang berkomunikasi tersebut. Caranya? Dengan menggunakan perintah yang sederhana yaitu PING. Alternatif lainnya, anda bisa melakukan scanning lewat tab **Sniffer** pada bagian **Host** dan klik icon **+** (plus) maka akan keluar Mac Address Scanner :



Anda bisa memilih untuk mencentangi Promiscious-Mode Scanner untuk lebih spesifik mengenai ARP tiap-tiap komputer atau hanya sekedar scan biasa.

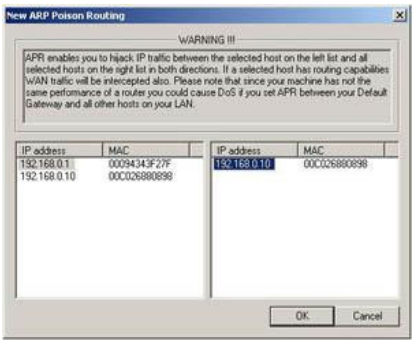
Nah, untuk memulai kegiatan ARP Poisoning, langkah-langkahnya adalah :

1. Buka Cain dan pilih kartu jaringan anda kemudian aktifkan sniffer dan APR (Icon nomor 2 dan tiga dari kiri, warna hijau dan kuning).
2. Pilih tab **Sniffer**, dan pada sub-tab **Host**, lakukan ping dengan command prompt atau tekan **insert** untuk melakukan scan terhadap komputer target jika data MAC maupun IP tidak diketahui
3. Klik sub-tab **APR**, klik bagian tengah yang ada putih-putihnya dan terbagi oleh table-tabel (maaf, saya tidak tahu namanya). Jika lokasinya benar, icon **+** (plus) yang berwarna biru akan bisa di klik.
4. Tekan tombol **insert** pada keyboard atau icon **+** (plus).

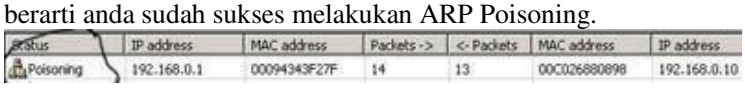


5. Pilih komputer yang ingin anda racuni pada jendela yang keluar. Perhatikan bahwa 2 komputer tersebut memang berkomunikasi (jika tidak, apa yang mau diendus?). Karena

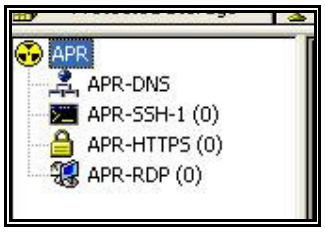
layer dari jendela tersebut terbagi dua, pilihlah dari jendela kiri komputer A, dan dari jendela kanan komputer B misalnya.



6. Jika langkah-langkah anda benar, pada status anda akan melihat tulisan *Poisoning* disertai icon, disusul *alamat IP*, kemudian *MAC*, daftar paket yang tertangkap, dan seterusnya. Ini berarti anda sudah sukses melakukan ARP Poisoning.



7. Sekarang fokuskan perhatian anda pada bagian kiri dan anda akan menemukan :



Pada daftar tersebut, jika ada paket yang tertangkap, maka angka dalam kurung (misalnya (0)) akan bertambah. Sebagai contoh, bila pada komputer target (komputer A) membuka situs hotmail melalui komputer B (misalkan komputer B adalah gateway) dan mengisi box Username dan Password pada situs hotmail, maka angka pada APR-HTTPS akan bertambah.

8. Kita misalkan APR-HTTPS bertambah. Maka yang perlu kita lakukan adalah mengklik APR-HTTPS.
9. Setelah anda mengkliknya, maka akan tampak 2 buah kolom. Kolom yang atas, adalah daftar sertifikat keamanan palsu yang dibuat oleh cain, dan kolom yang dibawahnya adalah daftar file log yang berhasil ditangkap.
10. Pilih file log yang anda rasa memiliki password, kemudian klik kanan dan pilih view. Sekarang anda bisa menganalisa log tersebut. Memang log yang ditampilkan berantakan, tapi yang perlu anda lakukan hanyalah analisa script yang sederhana. Misalnya mencari yang berhubungan dengan password dan username tentu dekat dengan login.
    Sebagai contoh, hasil tangkapan pada situs hotmail misalnya :
    ….login=blackdramon@msn.com&domain=passport.com&passwd=gantengsekali&sec=&mspp_shared=&padding=xxxx…..
    Berarti pada hotmail, target menggunakan user id *blackdramon@msn.com* dengan password *gantengsekali*.

❖ **Route Table Manager**

Fungsinya sama saja dengan fitur route.exe pada windows. Hanya saja tampilanya sudah menggunakan GUI jadi lebih enak dilihat. Anda tidak tahu route.exe? buka command prompt dan ketik *route* kemudian tekan enter. Pada cain, klik **tools** -> **Route Table**. Sebagai tambahan, route kira-kira berarti jalan dalam cara yang dilalui oleh paket data dalam sebuah jaringan saat proses routing.

❖ **SID Scanner**

Menemukan username yang berhubungan dengan SID (security identifier-tanda pengenal keamanan) dari sebuah remot, walaupun pada komputer yang mengaktifkan "RestrictAnonymous" (user anonyim tidak bisa membuka/mengakses). Sama seperti program **sid2user** buatan Evgenii B. Rudnyi Untuk menjalankannya klik kanan pada User target (dalam tab network) kemudian pilih pilihannya dari pop-up yang muncul.

❖ **Network Enumerator**

Menganalisa username, workgroup, apa-apa yang di sharing, serta servis lainnya yang berjalan pada komputer, kemudian anda bisa mengkliknya untuk melihat informasi yang lain. Cara membukanya? Klik tab **network** dan anda akan menemukan ini :


Inilah Network Enumerator.

❖ **Service Manager**

Membuat anda bisa menghentikan, memulai, atau melanjutkan servis yang terdapat pada komputer yang terdeteksi di Network Enumerator. Caranya? Klik **services** dan pada bagian kanan anda akan melihat daftar dari servis yang berjalan. Klik kanan saja. Untuk melakukan ini dibutuhkan akses administrator pada komputer yang di remote.

❖ **Routing Protocol Monitors**

Adalah kemampuan Cain untuk menangkap data yang lalu-lalang dari protokol-protokol routing. Saya rasa penjelasan ini sudah ada dalam sniffing, jadi termasuk fitur dari kemampuan Cain untuk melakukan sniffing, jadi tidak perlu dijelaskan deh… Lokasinya? Klik tab **sniffer** dan anda akan menemukannya pada sub-tab **Routing**.

❖ **Full RDP sessions sniffer for APR (APR-RDP)**

Membuat anda memiliki kekuasaan untuk mendapatkan semua data yang lalu-lalang pada protokol Remote Desktop, termasuk keystroke keyboardnya. Untuk melihatnya, cukup dengan LSA Secret Dumper yang sudah dijelaskan sebelumnya. Fitur ini termasuk fitur yang dijalankan saat APR Poisoning dilakukan, tertutama berkaitan dengan kegiatan menentukan signature palsu. Untuk itu, diperlukan pengetahuan dan pemahaman mengenai PPK Key. Untuk lebih Jelasnya, anda bisa melihat pada file help dari program Cain.

❖ **Full SSH-1 sessions sniffer for APR (APR-SSH-1)**

Termasuk fitur untuk menangkap data pada saat APR Poisoning dilakukan pada situs HTTPS, yaitu yang menggunakan sertifikat. Karena pokok bahasan mengenai APR Poisoning ada diatas, jika anda masih kurang jelas, silahkan Scroll Up. Poin tambahan disini adalah mengenai SSH. SSH, atau Secure Shell, adalah tanda bukti mengenai validitas keamanan dari sebuah situs ditengah jaringan yang tidak dipercaya.

Anda kurang paham? Begini, sama seperti tanda polisi yang sering dikeluarkan oleh polisi-polisi dalam film mafia Hongkong. Hanya dengan mengeluarkan tanda itu seklias, satu kampung akan percaya anda adalah polisi. Dengan mudah penjahat memalsukan tanda seperti itu, dan Begitupula dengan fitur Cain yang dengan mudah membuat sertifikat palsu sehingga korban percaya-percaya saja.

Nah, saat seseorang membuka sebuah situs yang terpercaya pada saat APR Poisoning dilakukan, Cain akan mengendus datanya, kemudian membuat yang palsu untuk diperlihatkan sebagai bukti bahwa SAYA ADALAH SERVER!

Untuk lebih jelasnya, berikut adalah rekonstruksinya :

- Client membuka SSH port pada server.
- Server yang melihat ada tamu pada port SSHnya, akan mengirimkan string identifikasi, yang kemudian dibalas pula dengan string identifikasi dari komputer Client.
- Server yang saying pada tamunya akan mengirimkan kunci enkripsi asymmetric dan informasi lain yang dibutuhkan kepada Client, dan sayangnya, disadap oleh Cain! Cain yang menyadap ini akan meneruskan ke Client, tapi sayangnya, kunci enkripsi asymmetric yang digunakan adalah milik Cain, bukan milik server lagi.
- Client yang menerima hadiah asymmetric dengan senang hati akan mengirimkan kunci enkripsi session yang dibutuhkan untuk menerjemahkan data-data yang nanti akan dikirim antara Server dan Client, dengan menggunakan kunci enkripsi asymmetric dari Cain.
- Client dan Server mulai berkomunikasi dengan menggunakan kunci enkripsi symmetric dan kunci enkripsi session. Merasa senang bahwa tidak ada yang bisa membaca paket data diantara mereka, padahal dua kunci tersebut terdapat pada Cain sehingga Cain bisa menerjemahkannya.

❖ **Full HTTPS sessions sniffer for APR (APR-HTTPS)**

Kemampuan Cain dalam menjalankan APR Poisoning melalui Man-In-The-Middle Attack. Tidak perlu dijelaskan lebih lanjut karena sudah dijelaskan sebelumnya.

❖ **Certificates Collector**

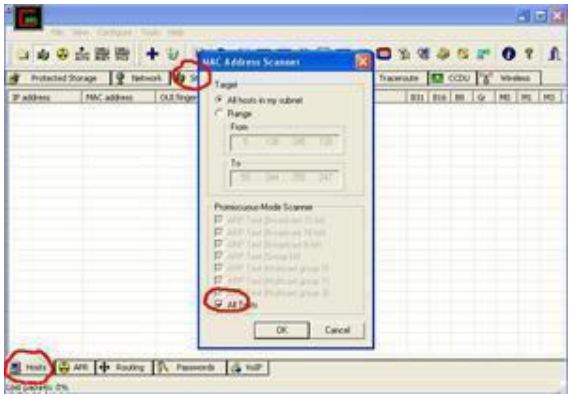
Pada situs yang menggunakan HTTPS, diperlukan sertifikat keamanan. Nah, saat melakukan ARP Poisoning otomatis sertifikat ini dibutuhkan. Cain memiliki kemampuan untuk mendapatkan sertifikat ini dari sebuah situs HTTPS dan menggunakannya dalam proses ARP Poisoning. Yang enak, anda juga bisa mengumpulkan sertifikat ini dari semua situs yang menggunakan sertifikat yang anda ketahui menjadi sebuah list untuk persiapan serangan Man-In-The Middle. Untuk manual, klik tab **Sniffer**, sub-tab **APR-HTTPS**, kemudian tekan tombol insert pada keyboard atau klik icon **+** (plus).

❖ **MAC Address Scanner with OUI fingerprint**

Kemampuan Cain dalam menemukan alamat MAC komputer dalam sebuah jaringan yang menggunakan Switch. Mengenai OUI Fingerprint, adalah semacam tanda tangan digital yang memberikan informasi mengenai vendor dari MAC-nya. Informasi mengenai vendor bisa berguna untuk cepat mengetahui mengenai switch, routers, load balancers dan firewall yang ada di LAN.

❖ **Promiscuous-mode Scanner based on ARP packets**

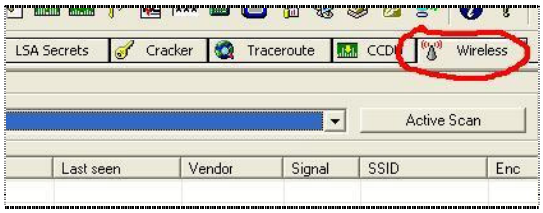
Adalah kemampuan Cain untuk melakukan scanning pada jaringan, sambil melakukan tes ARP. Mengaksesnya lewat tab **Sniffer**, Sub-tab **Hosts**, kemudian tekan tombol insert pada keyboard atau klik icon **+** (plus) pada Cain. Saat jendela baru muncul, beri saja tanda cek pada all test.



❖ **Wireless Scanner**

Kemampuan untuk melakukan Scan pada semua hotspot yang terdapat di sekitar anda menjadikan Cain adalah alat WarDriving yang baik. Memberikan detail mengenai alamat MAC, kapan terakhir kali servis aktif, para pengguna, kekuatan sinyal, nama dari jaringan, tipe jaringan dienkripsi tidaknya paket data, termasuk apakah tipe jaringan Ad-Hoc atau infrastructure, kanal-kanal aktif dalam jaringan, termasuk kecepatan akses jaringan tersebut. Dengan menggunakan AirCap adapter, passive scanning dan sniffing WEP IV bisa dilakukan. Semuanya dilakukan dengan meminta paket (packet request) dari hotspot.

Bisa diakses dengan mudah melalui satu kali klik pada tab **Wireless**. Tab yang paling kanan dari sudut pandang anda.

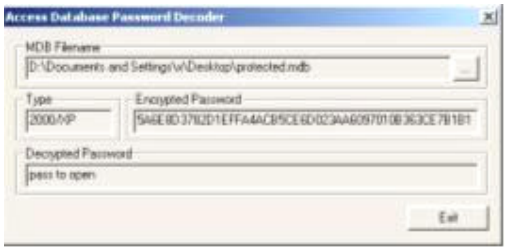


❖ **802.11 Capture Files Decoder**

Kemampuan Cain dalam mendecode file capture wireless Wireshark atau Airodump yang berisi frame enkripsi WEP atau WPA. Mengaksesnya? Klik tab **Cracker** dan pilih **Decode**.

❖ **Access (9x/2000/XP) Database Passwords Decoder**

Kemampuan cain dalam membuka file MDB yang di password yang dibuat dengan Microsoft Access 9x, 2000, atau XP dikarenakan kelemahan enkripsi XOR yang digunakan.



Untuk menggunakannya, klik **Tools**, kemudian pilih **Access Database Password Decoder**.

❖ **Base64 Password Decoder**

Mendecode password dalam enkripsi Base64. Base64 digunakan pada beberapa protokol standar internet. Yang perlu dilakukan hanyalah menangkap data yang dalam bentuk enkripsi tersebut, dan paste-kan data yang terenkripsi tersebut dalam kotak Base64 Password Decoder.

Untuk menggunakannya, klik **Tools**, kemudian pilih **Base64 Password Decoder**

❖ **Cisco Type-7 Password Decoder**

Mendecode password Cisco Type-7 yang digunakan pada file konfigurasi router dan switch (tidak bisa mendecode Cisco type-5) Untuk menggunakannya, klik **Tools**, kemudian pilih **Cisco Type-7 Password Decoder.**

❖ **Cisco VPN Client Password Decoder**

Mendecode password client Virtual Private Network dari connection profile (formatnya *.pcf). Ambil dari file tersebut (enc_GroupPwd or enc_UserPassword) kemudian pastekan pada jendela Cisco VPN Client Password Decoder. klik **Tools**, kemudian pilih **Cisco VPN Client Password Decoder**

❖ **VNC Password Decoder**

Virtual Network Computing adalah fitur remote desktop lewat internet yang Cross Platform, artinya beda tipe komputer tdak masalah. Nah, password VNC ini disimpan dalam komputer pada registry :

\\HKEY_CURRENT_USER\\Software\\ORL\\WinVNC3\\Password
atau
\\HKEY_USERS\\.DEFAULT\\Software\\ORL\\WinVNC3\\Password

Nah, yang perlu dilakukan tinggal membuka registry tersebut, kopi valuenya, dan dipastekan di decoder. Decoder sendiri dapat diakses melalui **Tools**, kemudian pilih **VNC Password Decoder**

❖ **Enterprise Manager Password Decoder**

Mendecode password Microsoft SQL Server Enterprise Manager (7.0 dan 2000). Sebagai info, password tersebut disimpan di registry pada key :

SQL2000: HKEY_CURRENT_USER\\Software\\Microsoft\\Microsoft SQL Server\\80\\Tools\\SQLEW\\Registered Servers X\\
Dan
SQL 7.0: HKEY_CURRENT_USER\\Software\\Microsoft\\MSSQLServer\\SQLEW\\Registered Servers X\\

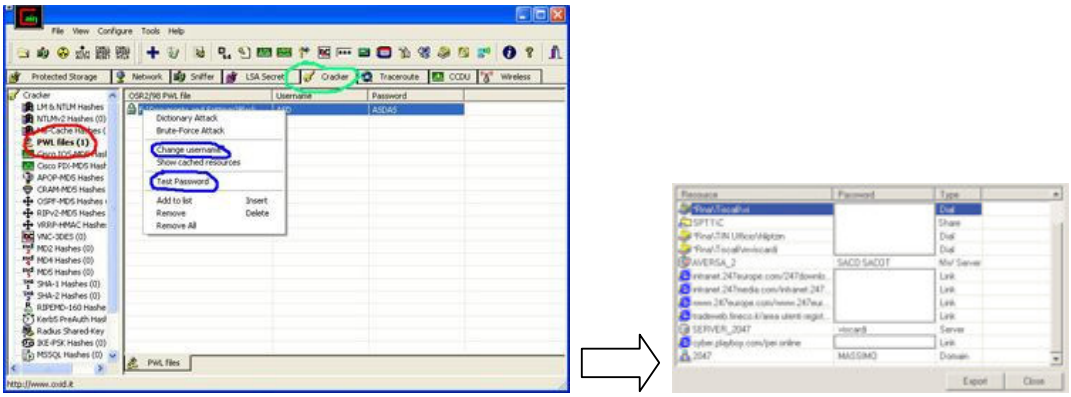
Decoder sendiri dapat diakses melalui **Tools**, kemudian pilih **Enterprise Manager Password Decoder**

❖ Remote Desktop Password Decoder

Mendecode password Remote Desktop Password Decoder (*.RDP). Decoder sendiri dapat diakses melalui **Tools**, kemudian pilih **Remote Desktop Password Decoder** (Hanya bisa dilakukan pada mesin yang sama dengan yang membuat file RDP karena file tersebut menggunakan CryptProtectData API pada mesin tersebut).

❖ PWL Cached Password Decoder

Anda yang pernah menggunakan windows 98 mungkin mengetahui sebuah tool administrasi bernama Password List Editor (PWLedit), dimana kita bisa melihat resource dari daftar password user, tanpa dapat melihat password sebenarnya. Cain juga mampu melakukannya dengan tambahan, passwordnya benar-benar terlihat. Kelemahannya hanya satu, yaitu anda wajib mengetahui password master PWL tersebut. Untuk membukanya, pilih tab **Cracker**, pada list sebelah kiri **PWL Files**, kemudian masukkan file PWL yang ada dengan menekan tombol **insert** pada keyboard atau icon **+** (plus) pada Cain. Setelah pwl tersebut masuk dalam daftar pada tabel sebelah kanan dari list tersebut, klik kanan pada nama file PWL tersebut, dan masukkan username dengan memilih *Change Username* dan masukkan password dengan memilih *test password*.



❖ Password Crackers

Saat anda sama sekali tidak tahu apa passwordnya, yang paling sering dilakukan adalah menebak apa kira-kira passwordnya. Menuliskan satu-persatu password yang kira-kira digunakan korban adalah hal yang membosankan, walaupun anda dijanjikan kenaikan gaji (naik pangkat dua

tingkat sih oke-oke aja…). Nah Cain bisa mempermudah dengan fitur tebak-tebakan otomatis yang disebut Password Cracker. Saat anda membuka tab **Cracker** dan mengklik list **Cracker**, anda bisa mengklik kanan daftar file yang dipassword dan memilih menggunakan cracker apa.

Ada dua tipe penebak-nebakan yang paling sering digunakan, yaitu *Dictionary attack,* yaitu menyusun sebuah daftar mengenai kemungkinan password yang digunakan, kemudian program cracker akan mencobanya satu-persatu. Pada cain, untuk menambahkan daftar dictionary atau kamus, bisa dengan memnyusunnya sendiri atau mendownload kamus yang banyak bertebaran di internet. File yang biasa digunakan biasanya berformat *.txt. Untuk menggunakan file kamus tersebut, setelah anda menglik kanan pada file dalam daftar cracker cain dan memilih dictionary attack, pada menu yang keluar, pilih saja **add.**

Pada options, anda bisa memilih bagaimana list tersebut digunakan, misalnya termasuk mengecek apakah kata-kata dalam kamus tersebut digunakan terbalik dan sebagainya. Hanya saja, semakin banyak yang anda centengi, pekerjaan akan semakin lama. Dictionary attack memang terkenal sebagai yang paling makan harddisk. Jika anda mengumpulkan semua kata-kata dan kombinasi di dunia ini, walaupun dalam format text, tidak akan ada harddisk yang sanggup menampungnya, sekiranya hingga hari ini. Untuk itu, diciptakanlah *Brute Force Attack*

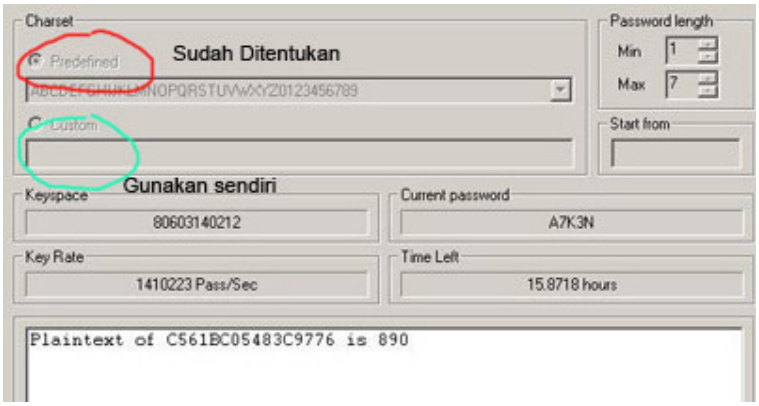
Brute Force Attack atau serangan Kasar, yaitu mencoba semua kombinasi besar kecil huruf dan angka serta symbol pada keyboard. Memang hemat harddisk, tapi sangatlah lama prosesnya. Saya pernah mencoba untuk membuka password yang terdiri dari lima kata dan angka, prosesnya sendiri memakan waktu sampai lima jam. Yah, semuanya tergantung kecepatan komputer anda tentu saja.

Saking rumitnya tehnik ini, sampe ada rumusnya, yaitu :

KS = L^(m) + L^(m+1) + L^(m+2) + ... + L^(M)

Dimana *L=Panjang Password (length), m=Panjang Minimum dan M=Panjang Maksimum.* Untuk lebih jelasnya mengenai penerapan rumus tersebut, mohon maaf, karena saya tidak bisa menjelaskan. Maklum, nilai rapor untuk matematika saya 5 karena saya paling sering tidur dikelas, sekaligus penyebab saya D-O.

Pada cain, untuk mengaksesnya sama saja seperti dictionary attack. Nah, pada cain sendiri ada dua pilihan, yaitu menggunakan kombinasi yang sudah disediakan, atau menggunakan custom combination.



Fitur custom ini biasanya digunakan jika anda tahu karakter apa saja yang kira-kira tidak digunakan dalam daftar password tersebut. Misalnya anda tahu bahwa password tersebut terdiri dari nama pacar si korban, yaitu *Diptaningsih*, tapi oleh korban diputar-balik (di scramble), misalnya, *ningsihdipta* atau *atpidnihisng* dan lain-lain. Nah, daripada anda coba semua kombinasi huruf, masukkan saja kata *Diptaningsih* dalam box custom. Masalah percobaan putar-putar itu urusannya si Cain.

Sebagai tambahan, dalam melakukan Brute Force, juga dikenal sebuah tehnik bernama Xieve™Attack, yaitu melakukan Brute Force, tapi mengesampingkan kombinasi-kombinasi yang tidak memiliki makna sama sekali.

❖ Cryptanalysis attacks

Tehnik Cryptanalysis yang dikenalkan oleh Philippe Oechslin (*Faster Cryptanalytic time – memory trade off*) adalah tehnik yang menggunakan tabel yang berisi password yang dienkripsi yang sudah dikalkulasikan sebelumnya. Tabel ini dikenal dengan nama Rainbow Tables. Tehnik ini adalah pengembangan dari tehnik trade-off yang mempercepat proses mendapatkan password. Software yang terkenal akan tehnik ini adalah *RainbowCrack* yang dibuat oleh Zhu Shuanglei. Untuk mengaksesnya sama seperti diatas, kemudian pilih **Cryptanalysis attack**. Untuk memperdalam mengenai Cryptanalysis Attack dan Rainbow Tables, anda bisa mengunjungi : http://en.wikipedia.org/wiki/Rainbow_table

❖ WEP Cracker

Mendpatkan kunci WEP dengan memanfaatkan kelemahan tehnik enkripsi RC4. Tehnik ini sendiri gagal bila jaringan menggunakan Dynamic WEP.

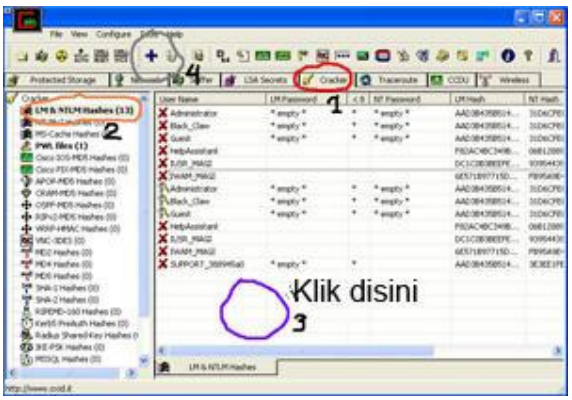
❖ Rainbowcrack-online client

Meng-Crack password dengan mengakses RainbowTable yang sudah dijelaskan diatas melalui internet. Anda bisa menemukan pilihan untuk melakukan ini dengan cara seperti yang

sudah disebutkan diatas yaitu mengklik kanan pada file yang terdapat pada list dan memilih **Rainbowcrack-online**.

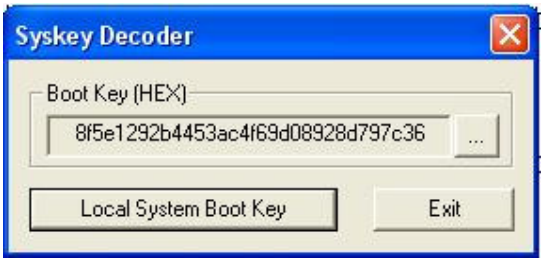
❖ **NT Hash Dumper + Password History Hases (works with Syskey enabled)**

Mendapatkan password hash NT dari file SAM, biarpun syskey di aktifkan atau tidak. Tehnik yang digunakan adalah DLL Injection, sama seperti **Credential Manager Password Decoder.** Untuk mengaksesnya, pilih tab **Cracker**, dan pada list sebelah kiri, pilih **LM & NTLM Hashes**. Klik tabel kanannya, kemudian tekan **insert** di keyboard atau icon **+** (plus).

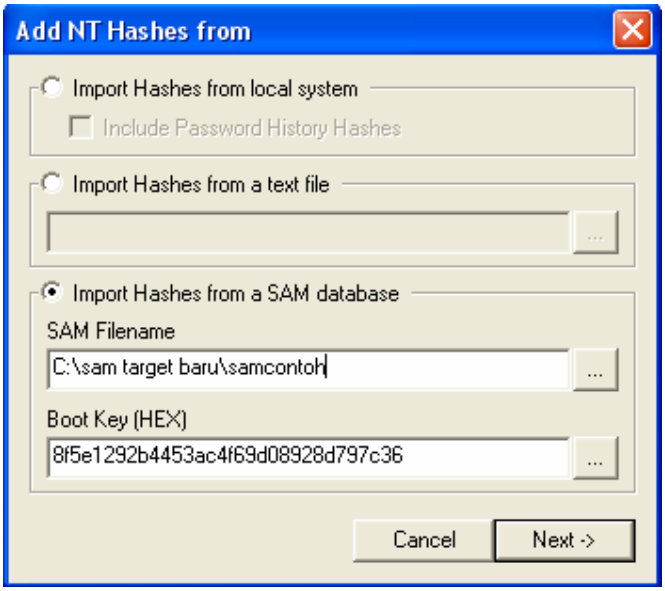


❖ **Syskey Decoder**

Membuka semua Boot Key yang digunakan oleh Syskey dari registry computer atau file off-line system. Boot Key apaan sih? Boot Key adalah kunci informasi yang disimpan oleh program syskey (syskey.exe) untuk melakukan enkripsi sebelum disimpan kedalam database SAM. Nah, jika disimpan di local, Boot Key akan diacak dalam subkey-subkey pada *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LsaSyskey,* kemudian Syskey Decoder akan menyusunnya kembali dalam bentuk heksadesimal dan siap dibaca dengan menggunakan **NT Hashes Dumper**. Untuk mengaksesnya klik **Tools** kemudian pilih **Syskey Decoder.**



Untuk mengambilnya langsung dari computer yang dipasangi Cain, cukup dengan mengklik *Local System Boot Key* atau anda bisa mengklik tanda titik tiga kali (…) untuk mengambilnya dari file registry yang sudah disimpan. Jika sudah didapatkan, yang perlu anda lakukan adalah mengakses **NT Hashes Dumper** yang sudah dijelaskan sebelumnya, memilih **Import Hashes From a SAM database**, memilih file samnya, kemudian paste-kan **Bootkey** dan hantam Next->.



gambar : mengimport SAM

❖ **MSCACHE Hashes Dumper**

Memperlihatkan semua hash dari password MSCACHE yang disimpan dalam registry. Fitur ini bisa anda temukan di list kiri pada tab **Cracker**.

❖ **Wireless Zero Configuration Password Dumper**

Memperlihatkan semua password Wireless Zero Configuration yang disimpan pada komputer. Untuk mengaksesnya, klik tools dan pilih saja **Wireless Password Dumper**, atau **alt+w**, atau klik ikon monitor hijau yang mengeluarkan sinyal nomor empat dari kanan anda.

❖ **Microsoft SQL Server 2000 Password Extractor via ODBC**

Mengkonekkan dirinya kedalam Server SQL (Microsoft SQL Server 2000 saja) melalui ODBC, dan menarik semua password yang ada dari database master. Untuk mengaksesnya, klik tab **Cracker** kemudian pada list sebelah kiri, pilih **MSSQL Hashes.**

❖ **Oracle Password Extractor via ODBC**

Mengkonekkan dirinya kedalam Server Oracle melalui ODBC dan menarik semua password yang ada dari database. Untuk mengaksesnya, klik tab **Cracker** kemudian pada list sebelah kiri, pilih **Oracle Hashes.**

❖ **MySQL Password Extractor via ODBC**

Mengkonekkan dirinya kedalam Server MySQL melalui ODBC, dan menarik semua password yang ada dari database. Untuk mengaksesnya, klik tab **Cracker** kemudian pada list sebelah kiri, pilih **MySQL Hashes.**

❖ **Box Revealer**

Memprlihatkan semua password yang ditutupi menggunakan tanda asterisk (***). Fitur ini sama seperti program Revelationnya Sneadboy. Tehnik yang digunakan adalah DLL Injection. Fitur ini bisa diakses melalui **tools**, kemudian pilih **Box Revealer**.

❖ **RSA SecurID Token Calculator**

Kartu RSA SecurID banyak digunakan di kantor-kantor yang memiliki system keamanan yang canggih. Kecil, ringan, dan anti air. Nah, fungsi alat ini kira-kira mengganti kode akses ke sebuah system setiap 60 detik sehingga kode akses ini susah ditebak. Jadi, penggunanya pertama akan memasukkan nomor PIN, diikuti kode akses yang diregenerasikan oleh alat tersebut.

anda pernah melihatnya?

Nah, Cain mampu menebak angka apa yang keluar sebelum alat RSA mengeluarkannya. Kira-kira sama seperti minta nomor buntut ke dukun, hanya saja hasilnya 100% benar! Ahhh… Seandaninya saja nomor togel menggunakan RSA, pasti saya sudah kaya sekarang…

Oh ya, satu lagi. Untuk mengetahui kode akses yang akan keluar, diperlukan dua nomor, yaitu nomor seri dari alat RSA tersebut, dan kunci aktivasinya. Dua-duanya biasanya disertakan dalam disket atau CD dari vendor alat tersebut. Biasanya sih dalam disket, soalnya filenya kecil. Format file tersebut adalah *.ASC.

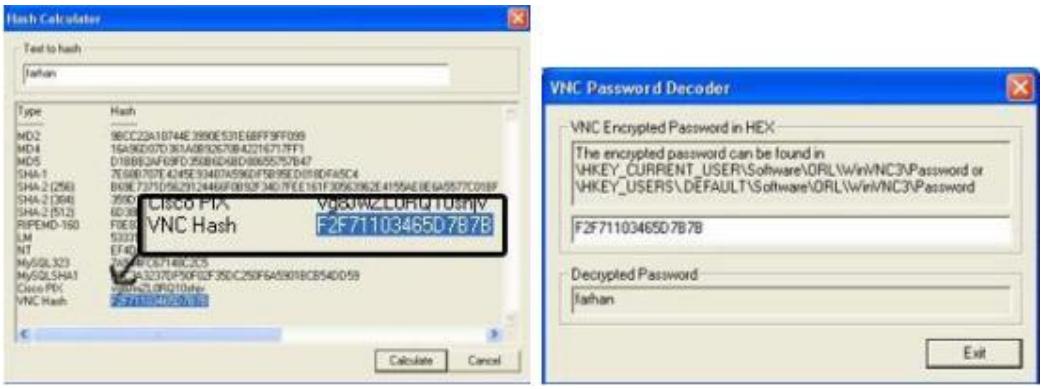
Bagaimana mendapatkannya seandainya perusahaan yang ingin diserang? Mudah, pacari saja karyawatinya dan minta langsung, atau lakukan Dumpster Diving (ngorek-ngorek tong sampah kantor orang buat nyari disket yang ada ASC-nya).

Fitur ini bisa diakses melalui **tools,** dan pilih **RSA SecureID Token Calculator**.

❖ **Hash Calculator**

Ini fitur yang menarik dari Cain menurut saya. Kita tinggal menuliskan sebuah teks, dan nilai hashnya, termasuk MD2, MD4, VNC, dan lain-lain, akan dimunculkan.

Sebagai contoh, saya menuliskan kata "farhan", semua nilai hashnya akan muncul, dan jika dicocokkan, saya contohkan dengan VNC, hasilnya akan sama.



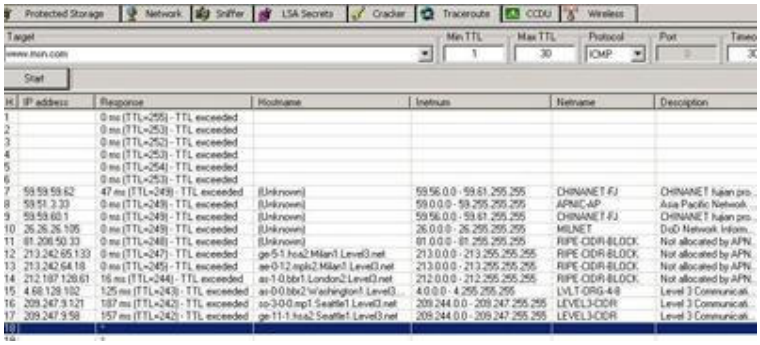
Fitur ini bisa diakses melalui **tools**, kemudian pilih **hash calculator**, atau kombinasi **ctrl+c**. Alternatif lain dengan mengklik icon nomor sepuluh dari kanan anda.

❖ **TCP/UDP Table Viewer**

Tools netstat ala Cain. Anda tidak tahu netstat? Coba ketikkan kata netstat pada command prompt dan semua aktivitas dari port-port pada komputer akan diperlihatkan. Fitur ini bisa diakses melalui **tools**, kemudian pilih **TCP/UDP Table**. Dengan alat ini, seperti menggunakan netstat, anda bisa mengetahui IP-Adress lawan Chatting anda. Misalkan anda menggunakan Yahoo Messenger, kirimkan sebuah file ke dia, dan buka TCP/UDP Table, dan lihat port mana yang aktif mengirimkan file tersebut. Disana pasti terdapat IP lawan Chatting anda. Untuk mengetahui informasi tambahan dari IP tersebut, pastekan saja IP tersebut pada situs-situs IP Resolver Service, misalnya di http://www.domainwhitepages.com.

❖ **TCP/UDP/ICMP Traceroute with DNS resolver and WHOIS client**

Windows memiliki software tracer bawaan yang bernama tracert.exe. Cara membukanya adalah dengan membuka command prompt dan mengetikkan tracert.exe. Cain sendiri memiliki tracer yang lebih baik dalam segi tampilan daripada windows. Lebih enak dilihat karena menggunaka GUI. Fitur ini bisa diakses melalui tab **Traceroute**. Masukkan nama situs yang ingin di trace pada kotak **Target,** pilih protokolnya, kemudian klik start, dan informasi mengenai situs tersebut akan ditampilkan, yang tentunya lebih enak dilihat daripada menggunakan tracer bawaan windows.



gambar : jendela TCP/UDP/ICMP Traceroute with DNS resolver and WHOIS client

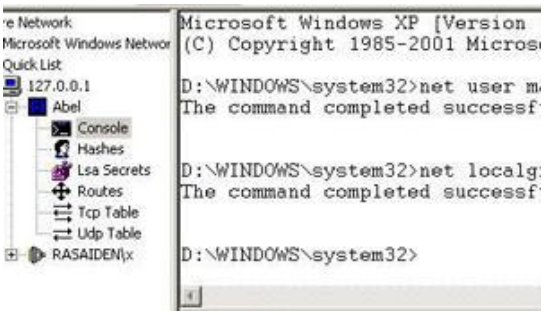
❖ **Cisco Config Downloader/Uploader (SNMP/TFTP)**

Kemampuan untuk mendownload atau mengupload file konfigurasi dari dan ke Cisco Devices lewat SNMP atau TFTP. Untuk informasi lebih lengkapnya, silahkan baca file help dari Cain.

Fitur-fitur Abel

❖ **Remote Console**

Melakukan remote console. Di setiap komputer dalam jaringan yang sudah dipasangi (atau "diinfeksi") abel, semua perintah console, atau dalam windows dikenal dengan command prompt, bisa dilakukan. Jika komputer yang terdeteksi dalam tab **network** sudah dipasangi able, maka icon abel akan muncul dan bisa di klik dan di expand kebawah. Anda akan menemukan icon **Console.** Klik saja, dan lakukan command prompt sesuka hati, sebagai administrator.



❖ **Remote Route Table Manager**

Sama seperti menggunaka route table manager yang sudah dijelaskan sebelumnya, hanya saja kali ini, data-data yang diperlihatkan dilihat dari sudut pandang komputer yang dipasangi (atau "diinfeksi") abel. Untuk mengaksesnya sama seperti melakukan remote console. Pilih icon

yang berhubungan dengan table manager pada icon-icon hasil expanded icon Abel pada komputer yang sudah dipasangi abel.

❖ **Remote TCP/UDP Table Viewer**

Melihat aktivitas dari port-port pada komputer yang dipasaning Abel. Cara mengaksesnya sama seperti diatas.

❖ **Remote NT Hash Dumper + Password History Hases (works with Syskey enabled)**

Melihat isi dari NT Hash pada komputer yang dipasangi Abel. Mengenai NT Hash Dumper sudah dijelaskan sebelumnya, dan cara mengaksesnya sama seperti diatas.

❖ **Remote LSA Secrets Dumper**

Melihat isi dari LSA pada komputer yang dipasangi Abel. Mengenai LSA Secret Dumper sudah dijelaskan sebelumnya, dan cara mengaksesnya sama seperti diatas.

Dengan kata lain, dengan menggunakan Abel, beberapa fitur yang dimiliki Cain bisa dijalankan pada komputer yang sudah dipasangi, diinfeksi, atau diremote oleh Abel. Sekarang anda mengerti mengapa mereka tidak saling membunuh tapi justru membantu anda.

☺

Biografi Penulis

Farhan Perdana. Drop out kelas 2 sma dan melanjutkan di sekolah terbuka. Belajar komputer secara otodidak.

Penulis dapat dihubungi melalui:
email : kuroiunagi@gmail.com
situs : http://aniplasma.co.nr